Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.082418

ARTICLE

Location Privacy Protection of Data Elements in ICVs: A Key Update Mechanism for Defending Against Chosen-Ciphertext Attacks

Lei Wang[1], Hongji Luo[2], Yong Heng[2], Jingnan Tang[2], Xiaochuan Ju[2], Jianwei An[1,*], Haitao Xu[1] and Xianwei Zhou[1]

[1]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China
[2]Beijing Institute of Electronic System Engineering, Beijing, China

*Corresponding Author: Jianwei An. Email: anjianwei@ustb.edu.cn

Received: 16 March 2026; Accepted: 22 April 2026; Published: 15 June 2026

ABSTRACT: In intelligent connected vehicles (ICVs) system, driving users connect to service providers (SPs) to obtain location-based services (LBS). Users transmit large volumes of encrypted sensitive information related to their itineraries to SPs to access value-added services. Attackers may launch chosen-ciphertext attacks (CCA) against SPs by exploiting the malleability of homomorphic encryption. This enables adversaries to infer or steal private key information, thereby threatening the long-term privacy of user data. Furthermore, existing key management technologies in ICVs system predominantly rely on passive defense strategies and suffer from limitations such as single protection mechanisms, delayed updates, and limited adaptability. To address these issues, this paper proposes an adaptive key update security mechanism based on a differential game framework. This mechanism treats the cumulative information leakage of the private key as a contested resource to construct a differential game model. Based on the feedback Nash equilibrium (NE), the mechanism adaptively derives the optimal homomorphic private key update frequency in response to the attack frequency, thereby maximizing the defense benefit. Finally, numerical simulations validate the correctness of the proposed model and demonstrate the effectiveness of the mechanism.

KEYWORDS: Intelligent connected vehicles (ICVs); data element privacy; differential game; adaptive key update; homomorphic encryption

1 Introduction

With the deep integration of 5G/6G technologies and intelligent connected vehicles (ICVs), vehicle-to-everything (V2X) networks have emerged as a cornerstone of intelligent transportation systems [1]. Location-based services (LBS) have evolved from simple navigational aids into essential services that support traffic analysis, collaborative perception for autonomous driving, and traffic flow scheduling [2]. To ensure service timeliness and accuracy, onboard terminals transmit trajectory data to service providers (SPs) at high frequencies. Such large volumes of location data serve as data elements in the ICVs ecosystem and provide a foundation for SPs to optimize algorithms and enhance quality of service (QoS) [3]. However, the exponential growth of data exchange between vehicles and SP driven by LBS has increasingly exacerbated concerns regarding data privacy leakage [4].

Location data inherently contain sensitive personal information. By analyzing vehicle trajectories, adversaries can infer users' home locations, workplaces, and behavioral patterns [5]. This paradigm assumes fully trusted SPs; however, in practice, SPs are often considered honest-but-curious, potentially inferring

private information during protocol execution. Moreover, SPs remain vulnerable to external attacks, which may lead to large-scale data breaches [6]. To balance data utility and privacy preservation, homomorphic encryption (HE) has attracted increasing attention. Notably, the Paillier cryptosystem supports additive operations over ciphertexts [7], enabling SPs to perform tasks such as traffic statistics and distance computation without accessing raw location data, thus preserving data utility while preventing direct exposure.

HE effectively isolates plaintext and establishes a protective barrier for ciphertext computation. However, most existing schemes overlook vulnerabilities caused by static key management [8]. Because schemes such as Paillier are malleable, they remain vulnerable to chosen-ciphertext attacks (CCA) [9]. In ICV environments, SPs may effectively serve as continuously online decryption or computation nodes, allowing attackers to analyze ciphertext responses and gradually accumulate private-key information over time [10]. Reusing a single public-private key pair over time significantly increases the risk of private key inference. Once compromised, previously encrypted data become vulnerable to retroactive decryption, undermining forward secrecy. Therefore, static encryption schemes are insufficient to ensure the long-term security of ICV data. To mitigate this risk, adaptive key update mechanisms are required to disrupt the attacker's information accumulation process. However, frequent key updates incur substantial computational and communication overhead, degrading system real-time performance, whereas infrequent updates fail to resist persistent chosen-ciphertext attacks (CCA). This results in a dynamic trade-off between system overhead and cumulative attack risk [11].

To address these challenges, this paper proposes a differential game-based adaptive key update mechanism for data circulation in ICV systems. Specifically, the cumulative information leakage of the private key is modeled as a state variable jointly controlled by both parties. The differential game captures the dynamic conflict between the attacker's information accumulation and the defender's key update actions. Both the defense strategy (key update frequency) and the attack strategy (CCA frequency) are incorporated into the optimization objective. The optimal defense strategy is analytically derived under the Nash equilibrium (NE) by solving the Hamilton-Jacobi-Bellman (HJB) equations. Compared with existing adaptive security approaches, such as reinforcement learning-based strategies and risk-sensing mechanisms, the proposed differential game-based method provides a fundamentally different modeling perspective. Specifically, RL-based methods rely on data-driven exploration and may suffer from convergence instability and local optima, while risk-sensing approaches typically depend on threshold-based feedback, leading to delayed responses under rapidly evolving attacks. In contrast, the proposed method models the attacker-defender interaction as a continuous-time dynamic game and derives the optimal key update strategy analytically via feedback Nash equilibrium. This enables predictive and globally optimal decision-making, thereby achieving faster convergence, stronger stability, and a more explicit characterization of the coupling between attack behavior and defense strategy. Overall, the main contributions of this paper are summarized as follows:

- We develop a differential game-based active defense model for data circulation in ICV systems, where cumulative private-key information leakage under homomorphic encryption is formulated as a continuous-time state variable. The model captures the dynamic interaction between CCA-based attacks and key update strategies, and characterizes the coupling among key update frequency, attack intensity, and data security.
- We propose a differential game-based adaptive key update (DG-AKU) algorithm. The algorithm derives the feedback NE of the game model by solving the HJB equations. Using the attack frequency and the current private-key leakage state, the algorithm adaptively computes the optimal key-update period.
- Extensive simulations compare DG-AKU with benchmark methods, including the adaptive risk-sensing strategy (ARSS) and an RL-based intelligent security mechanism (RL-IS). Results demonstrate superior

performance in convergence, steady-state defense effectiveness, and overhead efficiency. Sensitivity analyses on key parameters further validate the robustness of the proposed approach in ICV.

The remainder of this paper is arranged as follows: Section 2 presents relevant work. Section 3 outlines the system model. Section 4 derives the NE of the game model and proposes the DG-AKU algorithm. Section 5 presents simulation experiments to verify the validity of the model and the correctness of the NE solution. Finally, Section 6 concludes this paper.

2 Related Work

2.1 Location Privacy Protection Mechanisms in ICVs

Conventional location privacy preservation in the Internet of Vehicles (IoV) primarily relies on location perturbation, generalization, and pseudonymization. Reference [12] proposed an edge-assisted obfuscation and reporting control scheme based on clustering and k-anonymity, establishing a multi-level privacy protection framework at the system level. In [13], a tracking algorithm was developed to link vehicle pseudonyms across encrypted mix zones, mitigating inference-based location leakage. Reference [14] introduced a bi-layer privacy-preserving matching mechanism that combines noise injection and clipping for spatial obfuscation, and employs partial homomorphic encryption to construct distance-based encrypted preference lists, enabling differentially private stable matching. Furthermore, Reference [15] integrated federated learning with local differential privacy to design a collaborative transmission framework supporting privacy-preserving crowdsourcing applications.

Nevertheless, perturbation-based schemes often sacrifice data utility [16]. Noise injection and location obfuscation degrade data precision, making them inadequate for high-accuracy applications such as traffic analysis, billing, and collaborative perception in autonomous driving. To support high-fidelity data processing, cryptography-based privacy-preserving schemes have gained increasing attention. In [17], a privacy-preserving multidimensional data aggregation scheme was proposed, leveraging the Chinese remainder theorem (CRT) for data packing and secure key negotiation to ensure data integrity and authenticity.

This paper proposes using the update frequency of encryption keys as a defensive strategy by leveraging the usability without visibility property of the aforementioned HE technologies. This approach specifically addresses the vulnerability of static key management to long-term CCAs. The proposed strategy aims to adaptively derive an optimal key update mechanism that maximizes long-term privacy protection while preserving high data fidelity.

2.2 Homomorphic Encryption and Dynamic Key Management

Homomorphic encryption (HE) has been widely adopted in IoV for privacy-preserving computation due to its ability to support algebraic operations over ciphertexts. Reference [18] proposed a traffic flow prediction scheme based on the Paillier cryptosystem, enabling FL parameter aggregation without decrypting raw vehicle location data via its additive homomorphism. Reference [19] developed a homomorphic privacy-preserving aggregation protocol with low computational overhead, supporting fault tolerance, multi-category aggregation, and batch verification at both intermediate and central aggregators. However, despite achieving semantic security, partial homomorphic encryption schemes such as Paillier remain vulnerable to chosen-ciphertext attacks (CCA) due to their algebraic malleability. In vehicular environments, SPs may exploit ciphertext responses to accumulate side information and infer private keys [20].

Dynamic key management has become an important approach for mitigating key-compromise risks. Existing studies mainly focus on authentication credential renewal and lightweight key agreement mechanisms to improve security and efficiency. In addition to adaptive defense and key management approaches, recent studies have explored secure communication protocols for connected autonomous vehicles. Reference [21] focused on designing robust communication mechanisms to defend against various network-level attacks and ensure data integrity and authentication. These approaches primarily operate at the protocol level, emphasizing secure message exchange and communication reliability. In contrast, our work addresses the problem from a complementary perspective by modeling the long-term interaction between attackers and defenders and optimizing key update strategies to mitigate cumulative privacy leakage under CCA threats. Reference [22] proposed an attribute-based pre-authenticated communication protocol for 5G NR V2X, enabling online credential renewal to mitigate key leakage. Reference [23] introduced a lightweight authentication and key agreement scheme for smart grids, enhancing security while eliminating key escrow. Despite these advances, existing key update mechanisms largely rely on static periodic or event-driven strategies, failing to capture long-term attacker behavior [24]. Such static defenses are insufficient in IoV environments, where attacker-side information accumulates over time, progressively weakening system security.

To address this limitation, this paper leverages differential game theory to redesign the key management mechanism against CCA. The proposed approach adaptively determines the optimal private key update frequency based on real-time attack intensity, achieving a balance between system overhead and privacy protection by disrupting the attacker's information accumulation process.

2.3 Dynamic Defense Modeling Based on Differential Games

Security mechanisms in the IoV have evolved from static configurations to dynamic adaptive paradigms to counter increasingly sophisticated cyberattacks. Reference [25] proposed the adaptive risk-sensing strategy (ARSS), which enables continuous risk and trust assessment through real-time monitoring of multidimensional environmental indicators, allowing dynamic adjustment of security policies. Reference [26] developed an RL-based intelligent security (RL-IS) framework, in which agents learn optimal defense strategies via iterative interactions with the environment, improving decision-making under uncertainty.

However, these approaches are limited in addressing private key leakage in homomorphic encryption, which evolves as a continuous, accumulative state rather than discrete events. Differential game theory provides a principled framework for modeling continuous-time adversarial interactions between attackers and defenders [27]. Reference [28] formulated a DDoS defense model to optimize honeypot deployment under varying attack intensities. Reference [29] proposed a flow-level differential game to determine optimal activation and recovery strategies for compromised devices. In the vehicular domain, Reference [30] developed a non-cooperative computation offloading game for joint resource optimization, while Reference [31] studied distributed equilibrium-seeking methods for aggregative games with differential privacy guarantees.

Although differential games have been applied to resource scheduling and propagation control, they have not been used for decision-making on key update frequency because this problem involves long-term security state accumulation. This paper constructs an adaptive key update model by leveraging the ability of differential games to incorporate feedback from dynamic participant states. The proposed model adaptively updates the defense frequency to counter CCA by responding to evolving attack intensity. Ultimately, the proposed model achieves a balance between privacy preservation and resource utility by optimizing key update decisions over time. Recent studies have also explored advanced secure communication frameworks for connected and autonomous vehicles (CAVs). However, such approaches primarily focus on cryptographic robustness and secure data exchange, whereas the proposed DG-AKU framework addresses the dynamic

interaction between attackers and defenders by optimizing key update strategies over time, thereby providing a complementary perspective on adaptive security management.

The proposed approach differs from existing adaptive defense methods in two main aspects. First, unlike RL-based methods that learn policies iteratively, our framework derives closed-form equilibrium strategies, improving interpretability and computational efficiency. Second, unlike risk-sensing approaches that react passively to observed indicators, the differential game formulation captures the forward-looking interaction between attacker and defender, enabling proactive defense decisions under time-varying attacks.

Compared with the existing key update approaches, most prior studies focus on static or rule-based update strategies, where the update frequency is predetermined or adjusted based on limited system indicators. These methods generally do not explicitly model the dynamic interaction between attackers and defenders, nor do they capture the continuous evolution of system security risk under adaptive attacks. In contrast, the proposed method formulates the key update problem as a differential game, in which the attack behavior, system state evolution, and defense strategy are tightly coupled. This enables the service provider to adaptively adjust the key update frequency according to the real-time security state, thereby achieving a more effective balance between security and system overhead.

2.4 Limitations of State-of-the-Art Approaches

Existing key management systems usually support periodic key updates but often fail to adapt to evolving attacks. Most rely on static models that do not capture long-term adversarial dynamics. For example, risk-sensing methods react through fixed thresholds, and existing systems generally do not model the continuous-time interaction between attackers and defenders. These gaps are particularly problematic in scenarios where long-term privacy preservation is required, as attackers can exploit static strategies over time, leading to compromised security.

From the perspective of novelty positioning, the proposed method differs from existing approaches in three key aspects. First, adversarial learning and reinforcement learning-based defense methods typically rely on data-driven policy learning, which may suffer from convergence instability and limited interpretability in highly dynamic attack environments. Second, existing adaptive cryptographic key rotation schemes are generally designed as periodic or event-triggered mechanisms and do not explicitly model the attacker's strategic adaptation or the continuous accumulation of private-key leakage. Third, although game-theoretic cybersecurity models have been widely applied to problems such as DDoS defense and resource allocation, they rarely consider key update decisions under homomorphic encryption with long-term CCA threats. In contrast, the proposed method formulates cumulative private-key leakage as a continuous-time state variable and derives closed-form feedback Nash equilibrium strategies for adaptive key updates. This enables a principled balance between long-term privacy protection and system overhead, which is not explicitly addressed in existing work.

3 System Model

In this section, we construct a service provider-side data element defense model for the ICVs. Specifically, the first subsection presents an overview of the system architecture. The second subsection elaborates on the system model.

3.1 System Overview

As illustrated in Fig. 1, the ICVs system comprises a trusted authority (TA), user vehicle, and SPs. The TA is considered fully trusted, as it manages key distribution and oversees the system's operations. SPs and

vehicles, however, are treated as semi-trusted entities. SPs are responsible for processing encrypted data and providing services, but they may attempt to infer sensitive information. Vehicles, similarly, are trusted to securely store their keys and transmit encrypted data but remain vulnerable to specific attack vectors. The interaction between these semi-trusted entities is critical to the security model, as it ensures that privacy is preserved despite potential adversarial behaviors from some entities.

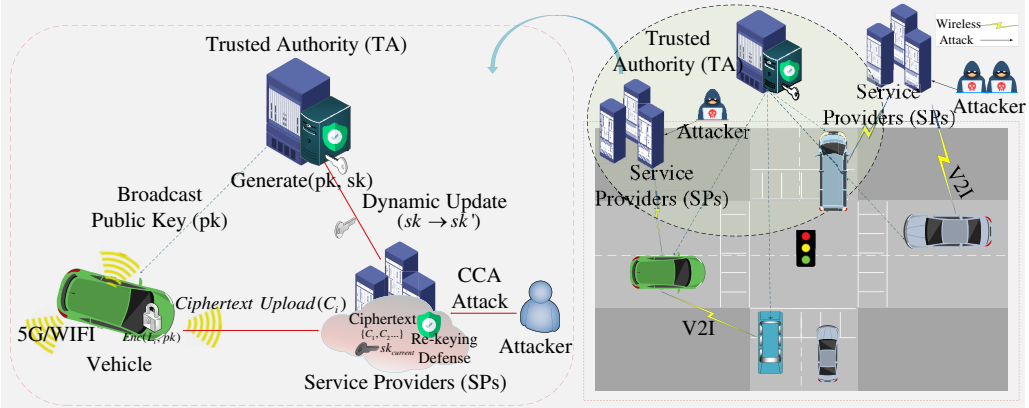

Figure 1: The structure diagram of the ICVs.

The TA authorizes and authenticates both service providers and driver users to ensure the legitimacy of network entities. User vehicles transmit data containing sensitive information, such as location coordinates, to service providers to access value-added services. In practical ICV deployments, the assumption that the SPs may act as a decryption oracle corresponds to scenarios where decryption-related operations are indirectly exposed through service interfaces, such as data processing application programming interfaces (APIs) or query-response mechanisms. In such cases, attackers may exploit adaptive queries to infer sensitive information from system responses, thereby approximating a CCA setting. Moreover, this assumption is consistent with an honest-but-curious or partially compromised SPs model, where the SPs correctly executes protocols but may unintentionally or maliciously expose information through repeated interactions. Attackers execute CCA against SPs to infer private keys and exfiltrate data, thereby causing privacy breaches. Consequently, the TA orchestrates adaptive private key updates to withstand chosen-ciphertext attacks and safeguard vehicular data uploaded to SPs. Table 1 summarizes the model parameters. Here, T_{att} denotes the attack cycle, i.e., the average time required for an attacker to compromise the current private key, and T_{upd} denotes the key update cycle. Their corresponding normalized decision variables are the attack frequency $f_{att}(t) = \frac{1}{T_{att}}$ and the key update frequency $f_{upd}(t) = \frac{1}{T_{upd}}$, respectively.

Table 1: Parameter description.

Parameters	Notation
The unlock key cycle	T_{att}
The key update cycle	T_{upd}
The cumulative information leakage of private key	$x(t)$
The impact factor of attack frequency on status	ω_1
The impact factor of update frequency on status	ω_2
The natural decay coefficient	δ
The risk of private key privacy leakage	θ

(Continued)

Table 1 (continued)

Parameters	Notation
The information reward discount factor	∂_1, ∂_2
The attack damage multiplier	α_1
The unit attack cost	C_1
The defense yield discount factor	α_2
The unit update cost	C_2
The unit transmission cost	C_3
The cost discount factor	γ

This paper proposes a differential game-based adaptive key update security defense mechanism. Its working principle is illustrated in Fig. 2. The detailed procedure is described as follows.

- During system initialization, the TA executes the Paillier key generation algorithm to generate the initial public-private key pair (pk_0, sk_0) for the first cycle. The TA broadcasts the public key pk_0 to vehicles and transmits the private key sk_0 to SPs.
- The TA continuously monitors decryption-oracle queries through the attack-frequency sensing module. Meanwhile, SPs deliver location-based services to vehicles.
- The attack-frequency sensing module estimates the average time T_{att} required for an attacker to compromise the current key. This estimation is obtained by statistically analyzing decryption requests per unit time and incorporating historical data. In practice, the attack frequency is not directly observable but can be estimated through statistical monitoring of abnormal decryption-related activities. Specifically, the system records the frequency of decryption requests, failed authentication attempts, and other security-related events over time, and combines them with historical attack data to estimate the average attack cycle T_{att}. The attack frequency is then obtained as $f_{att}(t) = \frac{1}{T_{att}}$, which serves as an input to the game-theoretic model.
- The strategy optimization module computes the optimal key update frequency $f_{upd}(t)$ by reading the real-time attack frequency T_{att} and issues instructions to the key generation module to initiate key regeneration. Here, $f_{upd}(t) = \frac{1}{T_{upd}}$. T_{att} represents the key update cycle.
- Upon receiving the instruction, the key generation module executes the Paillier key generation algorithm to select new large prime numbers and generate a new public key pk_{new} and private key sk_{new} for the next cycle. The module marks the new private key as pending activation.
- The TA encapsulates the new private key sk_{new} in an encrypted message and transmits it to service providers via a secure channel, while simultaneously broadcasting the new public key pk_{new} to all vehicles in the IoV.

The TA requires SPs to activate a dual-key coexistence mechanism to prevent service interruptions during the key-switch process. Specifically, ciphertexts generated before the key switch can still be decrypted and processed using the old private key, whereas newly uploaded ciphertexts are handled under the new key pair. This overlapping transition avoids service interruption and ensures continuous processing during the key switching period. SPs destroy the old private key after all legacy ciphertexts are processed to complete the defense loop.

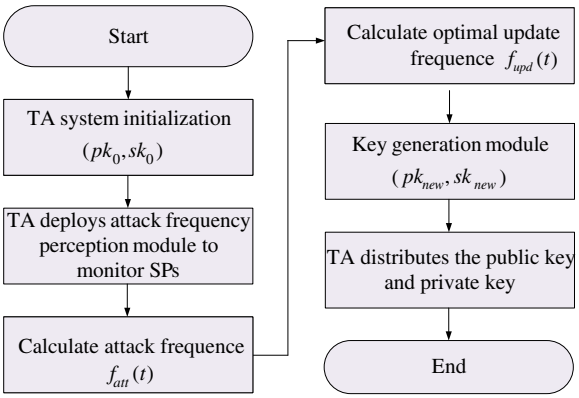

Figure 2: Mechanism flowchart.

Within the proposed defense mechanism, the TA employs the Paillier cryptosystem to encrypt plaintext and generate fresh public-private key pairs [32]. The steps are as follows.

- Key Generation. The large prime numbers, p and q, are randomly selected to satisfy the condition $\gcd(pq, (p-1)(q-1) = 1)$. The modulus $n = p \cdot q$ and $\lambda = \mathrm{l\,cm}(p-1, q-1)$ are subsequently computed. The function $H(u) = \frac{u-1}{n}$ is defined, and a generator g is randomly selected from the set $Z^*_{n^2}$ to ensure that the condition $\gcd\left(L\left(g^{\lambda} \bmod n^2\right), n\right) = 1$ is satisfied. To simplify the decryption computation, the parameter $\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n$ is calculated. Ultimately, the public key is generated as $pk = (n, g)$, and the private key is designated as $sk = (\lambda, \mu)$.
- Encryption. A random value $m \in Z_n$ is selected for any arbitrary plaintext message $r \in Z^*_n$ to satisfy the conditions $r < n$ and $\gcd(r, n) = 1$. Subsequently, the ciphertext c_m is computed. $c_m = E(m, pk) = g^m \cdot r^n \bmod n^2$.The c_m is given by

$$c_m = E(m, pk) = g^m \cdot r^n \bmod n^2. \tag{1}$$

- Decryption. The receiver possessing the private key $sk = (\lambda, \mu)$ recovers the plaintext by utilizing the following formula based on the Paillier decryption principle. The formula is given by

$$m = D(c, sk) = H\left(c^{\lambda} \bmod n^2\right) \cdot \mu \bmod n. \tag{2}$$

- Homomorphic property of encryption. The following relationship is satisfied given two ciphertexts $c_1 = E(m_1)$ and $c_2 = E(m_2)$

$$c_1 \cdot c_2 \bmod n^2 = E(m_1 + m_2 \bmod n). \tag{3}$$

3.2 Game Theory Model

In the proposed system model, an excessively high key update frequency incurs high computational and communication overheads. Conversely, attackers are afforded sufficient time to compromise keys and execute attacks when the key update interval is prolonged. Consequently, the private key update frequency of SPs is adjusted adaptively according to the observed attack frequency to balance security and system overhead.

Definition 1: *Cumulative information leakage of the private key $x(t)$. The state variable $x(t)$ at the SPs is defined as the cumulative information leakage of the private key, with a value range of $[0, 1]$.*

In the proposed model, the defender adaptively adjusts the key update frequency to mitigate CCA. As illustrated in Fig. 3, the security of the homomorphic private key at SPs is modeled as a temporal interaction

between the attacker and the defender. The downward trajectory represents the progression of time and attack evolution, while the dashed boundary denotes the critical threshold at which the private key is compromised. The attack duration is denoted by T_{att}, reflecting the finite time required to execute chosen-ciphertext attacks. To prevent key compromise, the defender must complete key updates within this attack cycle, i.e., regenerate and distribute new keys before the attack succeeds. Accordingly, the security condition is given by $0 \leq T_{upd} \leq T_{att}$.

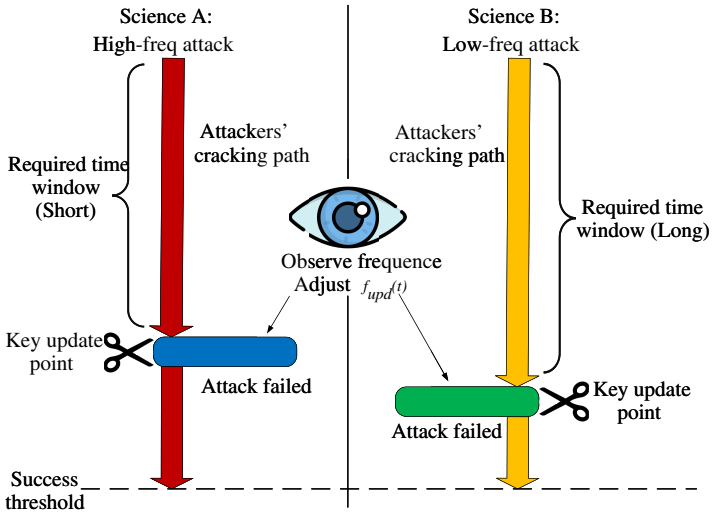

Figure 3: Key update security defense.

In the proposed model, the service provider's decision process is driven by the evolution of the system security state, rather than by a separate trust variable. Specifically, the cumulative information leakage of the private key, denoted by $x(t)$, characterizes how much security risk has accumulated over time under continuous attack. As $x(t)$ increases, the likelihood of private key compromise becomes higher, which reduces the defender's utility and prompts the service provider to increase the key update frequency. In the high-frequency attack scenario, accelerated information accumulation shortens T_{att}, prompting the defender to advance the update threshold and adopt a short key lifespan T_{upd}. In the low-frequency attack scenario, slower accumulation extends T_{att}, allowing the defender to delay updates and adopt a longer T_{upd} for improved resource efficiency.

To facilitate analytical tractability and ensure comparability between attack and defense strategies, the frequencies are normalized with respect to their respective maximum achievable values. This normalization constrains the control variables within a bounded range and allows the system dynamics to be analyzed on a unified scale. Among them, $f_{att}(t) = \frac{f_{att_t}(t)}{f_{att_{\max}}(t)}$. $f_{att_t}(t)$ represents the attacker's actual attack frequency at time $t(t \in [t_0, T])$, whereas $f_{att_{\max}}(t)$ denotes the maximum achievable attack frequency over the entire game horizon. Similarly, the defense strategy is normalized as $f_{upd}(t) = \frac{f_{upd_t}(t)}{f_{upd_{\max}}(t)}$. $f_{upd_t}(t)$ denotes the defender's actual key update frequency at time t, whereas $f_{upd_{\max}}(t)$ represents the maximum achievable defense frequency within the game duration. Let $x(t) \in [0,1]$ denote the cumulative information leakage of the private key at time t, where $x(t) = 0$ means no leakage and $x(t) = 1$ indicates complete compromise. The attacker controls the attack frequency $f_{att}(t)$, while the defender controls the key update frequency $f_{upd}(t)$. Moreover, ω_1 and ω_2 denote the impact factors of the attack frequency and update frequency on the state evolution, respectively, and δ denotes the natural decay coefficient of the leakage state.

In the proposed differential game framework, the attacker and the defender interact through the system state rather than through direct control over each other's actions. Specifically, the attacker determines the attack frequency $f_{att}(t)$ which directly affects the evolution of the information leakage state $x(t)$. A higher attack frequency accelerates the accumulation of leakage, leading to a higher risk level. In response, the defender observes the state $x(t)$ and adjusts the key update frequency $f_{upd}(t)$ to mitigate the increasing leakage risk. Therefore, the attacker influences the defender's key update strategy indirectly through the state dynamics and the associated payoff functions, forming a tightly coupled attack-defense interaction. The SPs' state at time t is given by

$$dx(t) = f(t, x(t), f_{upd}(t), f_{att}(t))dt. \tag{4}$$

The attacker launches CCA against SPs, and the impact of these attacks on the cumulative private-key leakage is set to $\omega_1 f_{att}(t)$. The influence of the defender on the cumulative information leakage is represented by $\omega_2 f_{upd}(t)$. Furthermore, the impact of natural attenuation on the cumulative information leakage is denoted by $\delta x(t)$. The $x(t)$ is given by

$$\begin{cases} \dfrac{dx(t)}{dt} = \omega_1 f_{att}(t) - \omega_2 f_{upd}(t) + \delta x(t), \\ x(t_0) = x_0. \end{cases} \tag{5}$$

In practical ICV security management, the feedback Nash equilibrium derived from the above game formulation represents a dynamically adaptive key update mechanism. The service provider determines the key update frequency based on the current system state, which captures the cumulative information leakage of the private key. Meanwhile, the attacker adjusts its attack frequency accordingly. At equilibrium, both parties adopt strategies that are optimal responses to each other, and neither can improve their utility through unilateral deviation.

Definition 2: Risk level of private key leakage θ. The risk level of private key leakage at the SPs reduces the defender's utility and increases the attacker's gain by intensifying system vulnerability. This risk level θ is defined over the range $[0, 1]$ to facilitate quantitative assessment of system security.

For clarity, the payoff design uses the following parameters: ∂_1 and ∂_2 denote the discount coefficients associated with information leakage in the attacker's and defender's utilities, respectively; α_1 and α_2 denote the reward discount coefficients for attack and defense; C_1, C_2, and C_3 represent the unit attack cost, unit key update cost, and unit key transmission cost, respectively; and γ denotes the cost discount factor. The model parameters have clear physical interpretations in the context of ICV security management. Specifically, ω_1 and ω_2 denote the relative influence of attack intensity and defense effort on the evolution of cumulative private-key leakage, respectively, while δ characterizes the natural attenuation effect of the leakage state over time. Moreover, α_1 and α_2 reflect the reward sensitivity of attack and defense actions, which can be associated with practical resource expenditure such as computation and communication overhead in ICV systems. In practice, these parameters can be calibrated according to system security requirements, service latency constraints, and resource budgets.

For the attacker, CCA are executed to compromise encryption keys for data element exfiltration and the maximization of offensive gains. The payoff function of the attacker comprises three distinct components: (i) the gains derived from the cumulative information leakage of the private key; (ii) the direct rewards obtained from the attacks; (iii) the cost of launching the attacks. Consequently, the payoff function of the attacker is formulated as follows

$$J_{att} = X_{att}(x(t)) + W_{att}(f_{att}(t), f_{upd}(t)) - C_{att}(f_{att}(t)), \tag{6}$$

where $X_{att}(x(t)) = \partial_1 x(t)$ denotes the gains derived from the cumulative information leakage of the private key. ∂_1 represents the discount coefficient for information returns with a unit defined as GB. $W_{att}(f_{att}(t), f_{upd}(t)) = \left(f_{att}(t) - f_{upd}(t)\right) f_{att}(t)\,(1+\theta)\,\alpha_1$ signifies the rewards obtained from attacks. α_1 represents the discount coefficient for attack rewards with a unit defined as \$ per unit time. $C_{att}(f_{att}(t)) = C_1 \gamma f_{att}(t)$ denotes the total attack cost, where C_1 is defined as the unit attack cost with a measurement of GB per unit time. γ represents the cost discount coefficient with a unit defined as \$/GB.

Within the game horizon $[t_0, T]$, the attacker seeks to maximize the offensive utility. Consequently, the objective function of the attacker is formulated to maximize the total returns throughout the game duration, as expressed below

$$\begin{aligned} J_{ATT} &= \max_{f_{att}(t)} \int_{t_0}^{T} \{J_{att}\} e^{-r(t-t_0)} dt + g_1 x(T) e^{-r(T-t_0)} \\ &= \max_{f_{att}(t)} \int_{t_0}^{T} \left\{ \partial_1 x(t) + \left(f_{att}(t) - f_{upd}(t)\right) \cdot f_{att}(t)(1+\theta)\alpha_1 - C_1 \gamma f_{att}(t) \right\} e^{-r(t-t_0)} dt \\ &\quad + g_1 x(T) e^{-r(T-t_0)}. \end{aligned} \tag{7}$$

At time T, the terminal value associated with the state of algorithm influences is $g_i x(T)$, $g_i \geq 0$, $i \in \{1, 2\}$. The game discount rate is r.

For the defender, the key update frequency is dynamically adjusted to intercept attacks and safeguard data privacy and security. The defender's payoff function comprises four components: (i) gains from proactive defense; (ii) key update costs; (iii) key transmission costs; (iv) penalty costs associated with state loss. Accordingly, the defender's payoff function is formulated as follows

$$J_{upd} = W_{upd}(f_{upd}(t), f_{att}(t)) - C_{upd}(f_{upd}(t)) - C_{tra}(f_{upd}(t)) - X_{upd}(x(t)), \tag{8}$$

where $W_{upd}(f_{upd}(t), f_{att}(t)) = \left(f_{upd}(t) - f_{att}(t)\right) f_{upd}(t)\,(1-\theta)\,\alpha_2$ denotes the gains derived from proactive defense. α_2 represents the discount coefficient for proactive defense returns with a unit of \$ per unit time. $C_{upd}(f_{upd}(t)) = C_2 \gamma f_{upd}(t)$ signifies the total cost of key updates. C_2 is defined as the unit update cost measured in GB per unit time. $C_{tra}(f_{upd}(t) = C_3 \gamma f_{upd}(t)$ represents the key transmission cost. C_3 denotes the unit transmission cost with a measurement of GB per unit time. $X_{upd}(x(t)) = \partial_2 x(t)$ represents the cost incurred by the cumulative information leakage during key updates. ∂_2 signifies the discount coefficient for information returns with a unit of \$/GB.

Within the game horizon $[t_0, T]$, the defender seeks to maximize the defensive utility. Consequently, the objective function of the defender is formulated to maximize the total returns throughout the game duration, as expressed below

$$\begin{aligned} J_{UPD} &= \max_{f_{upd}(t)} \int_{t_0}^{T} \{J_{upd}\} e^{-r(t-t_0)} dt + g_2 x(T) e^{-r(T-t_0)} \\ &= \max_{f_{upd}(t)} \int_{t_0}^{T} \left\{ (f_{upd}(t) - f_{att}(t)) f_{upd}(t)(1-\theta)\alpha_2 - C_2 \gamma f_{upd}(t) - C_3 \gamma f_{upd}(t) - \partial_2 x(t) \right\} e^{-r(t-t_0)} dt \\ &\quad + g_2 x(T) e^{-r(T-t_0)}. \end{aligned} \tag{9}$$

At the core of the model, we assume accurate estimation of attack frequency and continuous-time attacker behavior. While these assumptions simplify the analysis and allow for the derivation of closed-form

solutions, they may not fully reflect real-world ICV environments. In practice, attack frequency estimation relies on indicators such as decryption request frequencies or failed authentications, which may not always be perfectly accurate due to network or sensor limitations. Furthermore, the assumption of continuous-time attacker behavior might not hold in real-world scenarios where attacks could be sporadic or discrete. Despite these limitations, the model provides a useful framework for understanding the general dynamics of key update strategies, and future work could extend this model to incorporate more realistic attack behaviors, such as through discrete-event simulations or stochastic models.

The current framework focuses on frequency-based attack-defense interactions and does not explicitly consider more sophisticated adversarial strategies, such as stealthy attacks or data-poisoning behaviors. In addition, the proposed model is developed at an abstract system level and does not directly incorporate practical cryptographic protocol implementations, such as hybrid TLS and homomorphic encryption schemes. Furthermore, system-level constraints, including communication latency, bandwidth limitations, and scalability in large-scale vehicular networks, are not explicitly modeled. Addressing these aspects is an important direction for future work to enhance the applicability of the proposed framework in real-world ICV systems. And the current model implicitly assumes that the attack frequency can be accurately estimated from system observations. However, in practical ICV environments, such observations may be affected by noise, delay, or partial observability. Incorporating uncertainty-aware mechanisms, such as stochastic state estimation or partially observable decision models, is an important direction for future work to enhance the robustness of the proposed framework.

4 Model Solving and Algorithm Design

4.1 Proof of Nash Equilibrium Existence

Theorem 1: *The differential game model* $G\left(f_{upd}(t), f_{att}(t), x(t), t\right)$ *within the system admits a saddle point over the game horizon* $[t_0, T]$.

Proof of Theorem 1: Based on the established differential game model, the following conditions hold.

- The state variable $\frac{dx(t)}{dt}$ is continuous and bounded on the state space $[0,1]$ and the corresponding control spaces.
- The instantaneous payoff functions J_{UPD} and J_{ATT}, as well as the terminal payoff function $g_i x(T)$, are continuous with respect to all state and control variables.
- The state and instantaneous payoff functions are linear with respect to the control variables, and the corresponding control sets are convex. □

These conditions satisfy the requirements of Kakutani's fixed-point theorem [33]. First, we define the strategy space for both the attacker and defender as convex sets, and we represent their best-response correspondence using a convex-valued correspondence. Kakutani's fixed-point theorem is then applied to this correspondence to show the existence of a Nash equilibrium in mixed strategies. Specifically, we prove that the set of best responses is convex and non-empty. We further show that the correspondence satisfies the conditions of Kakutani's theorem, including closedness and the property of having a fixed-point. This fixed-point corresponds to a set of strategies where neither the attacker nor the defender can improve their utility by unilaterally deviating from their chosen strategy, thus establishing the equilibrium. The geometric interpretation of this equilibrium is that both players are at the point where their strategies mutually optimize the system's objectives. Consequently, at least one NE exists for this differential game, which completes the proof of Theorem 1.

4.2 Model Solution

Based on the aforementioned game model and the objective functions of both participants, we derive the optimal strategies for the defender and the attacker. For the defender, the key update strategy $\left\{f_{upd}^{*}(t)\right\} = \{M(t,x), t \in [t_0, T]\}$ provides the feedback NE solution for game models Eqs. (5) and (9) [34], satisfying the Bellman equation as follows

$$-R_t(t,x) = \max_{f_{upd}(t)} \left\{ \left[\left(f_{upd}(t) - f_{att}(t)\right) f_{upd}(t)(1-\theta)\alpha_2 - (C_2+C_3)\gamma f_{upd}(t) - \partial_2 x(t) \right] e^{-r(t-t_0)} + R_x(t,x) \cdot \left(\omega_1 f_{att}(t) - \omega_2 f_{upd}(t) + \delta x(t)\right) \right\}, \tag{10}$$

$$R(T,x) = e^{-r(T-t_0)} g_2 x(T). \tag{11}$$

For the attacker, the attack strategy $\{f_{att}^{*}(t)\} = \{K(t,x), t \in [t_0, T]\}$ provides the feedback NE solution for game models Eqs. (5) and (7) by satisfying the Bellman equation formulated as follows

$$-L_t(t,x) = \max_{f_{att}(t)} \left\{ \left[\partial_1 x(t) + \left(f_{att}(t) - f_{upd}(t)\right) \cdot f_{att}(t)(1+\theta)\alpha_1 - C_1 \gamma f_{att}(t) \right] \cdot e^{-r(t-t_0)} + L_x(t,x)\left(\omega_1 f_{att}(t) - \omega_2 f_{upd}(t) + \delta x(t)\right) \right\}, \tag{12}$$

$$L(T,x) = e^{-r(T-t_0)} g_1 x(T). \tag{13}$$

The following expressions are obtained by taking the first-order partial derivatives of Eqs. (10) and (12) with respect to $f_{upd}(t)$ and $f_{att}(t)$

$$0 = \left[\left(2f_{upd}(t) - f_{att}(t)\right)(1-\theta)\alpha_2 - (C_2+C_3)\gamma \right] e^{-r(t-t_0)} - \omega_2 R_x(t,x), \tag{14}$$

$$0 = \left[\left(2f_{att}(t) - f_{upd}(t)\right)(1+\theta)\alpha_1 - C_1\gamma \right] e^{-r(t-t_0)} + \omega_1 L_x(t,x). \tag{15}$$

The optimal strategies for both participants in the game are formulated according to Eqs. (14) and (15), as expressed below

$$f_{upd}^{*}(t) = \frac{(C_2+C_3)\gamma + f_{att}(t)(1-\theta)\alpha_2}{2(1-\theta)\alpha_2} + \frac{\omega_2 R_x(t,x) e^{r(t-t_0)}}{2(1-\theta)\alpha_2}, \tag{16}$$

$$f_{att}^{*}(t) = \frac{C_1\gamma + f_{upd}(t)(1+\theta)\alpha_1}{2(1+\theta)\alpha_1} - \frac{\omega_1 L_x(t,x) e^{r(t-t_0)}}{2(1+\theta)\alpha_1}. \tag{17}$$

The following results are derived by rearranging Eqs. (16) and (17)

$$f_{upd}^{*}(t) = \frac{C_1\gamma - \omega_1 L_x(t,x) e^{r(t-t_0)}}{3(1+\theta)\alpha_1} + \frac{2(C_2+C_3)\gamma + 2\omega_2 R_x(t,x) e^{r(t-t_0)}}{3(1-\theta)\alpha_2}, \tag{18}$$

$$f_{att}^{*}(t) = \frac{(C_2+C_3)\gamma + \omega_2 R_x(t,x) e^{r(t-t_0)}}{3(1-\theta)\alpha_2} + \frac{2C_1\gamma - 2\omega_1 L_x(t,x) e^{r(t-t_0)}}{3(1+\theta)\alpha_1}. \tag{19}$$

Proposition 1: *The value functions of the defender and the attacker, denoted as $R(t,x)$ and $L(t,x)$ respectively, are formulated as*

$$R(t,x) = [A_2(t)x + B_2(t)] e^{-r(t-t_0)}, \tag{20}$$

$$L(t,x) = [A_1(t)x + B_1(t)]e^{-r(t-t_0)}. \tag{21}$$

The expressions for $A_2(t)$ and $A_1(t)$ are given by

$$A_2(t) = \frac{\partial_2}{\delta - r} + (g_2 + \frac{\partial_2}{r-\delta})e^{(r-\delta)(t-T)}, \tag{22}$$

$$A_1(t) = \frac{\partial_1}{r-\delta} + (g_1 - \frac{\partial_1}{r-\delta})e^{(r-\delta)(t-T)}. \tag{23}$$

Proof of Proposition 1: Based on the established differential game model, the following conditions hold. Based on the Eqs. (20) and (21), we get the derivation of t and x respectively

$$R_t(t,x) = [(A_2'(t) - rA_2(t))x + (B_2'(t) - rB_2(t))]e^{-r(t-t_0)}, \tag{24}$$

$$R_x(t,x) = A_2(t)e^{-r(t-t_0)}, \tag{25}$$

$$L_t(t,x) = [(A_1'(t) - rA_1(t))x + (B_1'(t) - rB_1(t))]e^{-r(t-t_0)}, \tag{26}$$

$$L_x(t,x) = A_1(t)e^{-r(t-t_0)}. \tag{27}$$

Using Eqs. (10), (12) and (24)–(27), we can get

$$\begin{aligned} &-\left[(f_{upd}(t) - f_{att}(t))f_{upd}(t)(1-\theta)\alpha_2 - (C_2 + C_3)\gamma f_{upd}(t) - \partial_2 x(t)\right]e^{-r(t-t_0)} \\ &- A_2(t)e^{-r(t-t_0)}(\omega_1 f_{att}(t) - \omega_2 f_{upd}(t) + \delta x(t)) = \left[(A_2'(t) - rA_2(t))x + B_2'(t) - rB_2(t)\right]e^{-r(t-t_0)} \end{aligned} \tag{28}$$

$$\begin{aligned} &-\left[\partial_1 x(t) + \left(f_{att}(t) - f_{upd}(t)\right)f_{att}(t)(1+\theta)\alpha_1 \quad - C_1\gamma f_{att}(t)\right]e^{-r(t-t_0)} \\ &- A_1(t)e^{-r(t-t_0)}(\omega_1 f_{att}(t) - \omega_2 f_{upd}(t) + \delta x(t)) = \left[(A_1'(t) - rA_1(t))x + B_1'(t) - rB_1(t)\right]e^{-r(t-t_0)} \end{aligned} \tag{29}$$

For Eqs. (28) and (29) to be hold, it should be satisfied that

$$\begin{cases} A'_2(t) - (r-\delta)A_2(t) = \partial_2, \\ A_2(T) = g_2, \end{cases} \tag{30}$$

$$\begin{cases} A'_1(t) - (r-\delta)A_1(t) = -\partial_1, \\ A_1(T) = g_1. \end{cases} \tag{31}$$

Using Eqs. (30) and (31), we can get

$$A_2(t) = \frac{\partial_2}{\delta - r} + \left(g_2 + \frac{\partial_2}{r-\delta}\right)e^{(r-\delta)(t-T)}, \tag{32}$$

$$A_1(t) = \frac{\partial_1}{r-\delta} + \left(g_1 - \frac{\partial_1}{r-\delta}\right)e^{(r-\delta)(t-T)}. \tag{33}$$

□

From Eqs. (18), (25), (32) and (19), (27), (33), we can get the optimal defense strategy $f^*_{upd}(t)$ and the attacker's strategy $f^*_{att}(t)$

$$f^*_{upd}(t) = \frac{C_1\gamma - \omega_1\left[\frac{\partial_1}{r-\delta} + \left(g_1 - \frac{\partial_1}{r-\delta}\right)e^{(r-\delta)(t-T)}\right]}{3(1+\theta)\alpha_1} + \frac{2(C_2+C_3)\gamma + 2\omega_2\left[-\frac{\partial_2}{r-\delta} + \left(g_2 + \frac{\partial_2}{r-\delta}\right)e^{(r-\delta)(t-T)}\right]}{3(1-\theta)\alpha_2}, \tag{34}$$

$$f_{att}^{*}(t)=\frac{(C_2+C_3)\,\gamma+\omega_2\left[-\frac{\partial_2}{r-\delta}+\left(g_2+\frac{\partial_2}{r-\delta}\right)e^{(r-\delta)(t-T)}\right]}{3\,(1-\theta)\,\alpha_2}+\frac{2C_1\gamma-2\omega_1\left[\frac{\partial_1}{r-\delta}+\left(g_1-\frac{\partial_1}{r-\delta}\right)e^{(r-\delta)(t-T)}\right]}{3\,(1+\theta)\,\alpha_1}. \tag{35}$$

We propose the DG-AKU to implement and evaluate the effectiveness of the proposed defense strategy. The service provider's strategy update is state-driven. Specifically, the optimal key update frequency $f_{upd}^{*}(t)$ is dynamically adjusted according to the evolution of the state variable, which captures the cumulative information leakage of the private key. As $x(t)$ evolves over time under the combined effects of attack and defense actions, the service provider updates its strategy accordingly to mitigate further leakage and maintain system security.

Before presenting the detailed algorithm, we briefly summarize the main procedure of the proposed dynamic key update strategy. First, the system initializes the relevant parameters and state variables. Then, the current system state, which reflects the cumulative information leakage, is observed and updated over time. Based on this state, the optimal attack and defense strategies are derived according to the feedback Nash equilibrium. Finally, the service provider dynamically adjusts the key update frequency according to the equilibrium strategy, forming a continuous state-driven decision process. Algorithm 1 presents the pseudo-code.

Algorithm 1: Differential game-based adaptive key update algorithm (DG-AKU)

Input: Enter the system parameters in Eqs. (5), (7) and (9).
Output: The optimal strategies $f_{upd}^{*}(t)$ and $f_{att}^{*}(t)$ for both parties.
1: Initialize system parameters ω_1, ω_2, δ, ∂_1, ∂_2, α_1, α_2, C_1, C_2, C_3, γ, g_1, g_2.
2: **for** $t = t_0$: T;
3: Determine the optimal update strategy $f_{upd}^{*}(t)$ based on Eq. (34);
4: Determine the optimal attack strategy $f_{att}^{*}(t)$ based on Eq. (35);
5: Determine the maximum benefits for both parties according to Eqs. (7) and (9);
6: **end for**
7: Return optimal strategy sets $\left\{f_{upd}^{*}(t), f_{att}^{*}(t)\right\}$.

Complexity analysis: While the overall time complexity of the DG-AKU algorithm is $O(n)$, the practical computational and communication overhead depend on various factors such as the frequency of key updates, the number of vehicles and service providers, and the attack strategy. Specifically, the computational overhead is concentrated in steps 3 through 5 of the algorithm, where the optimal strategies and maximum payoffs are computed based on closed-form analytical solutions. Each time step involves $O(1)$ complexity for computation, resulting in an overall time complexity of $O(n)$ for n time intervals. The communication overhead primarily involves the transmission of encrypted data between the SPs and the vehicles, and it increases linearly with the number of entities involved. These overheads are necessary to maintain the privacy-preserving and real-time nature of the algorithm, ensuring robust defense against evolving attacks.

5 Simulation and Performance Analysis

In this section, numerical simulations are conducted on the MATLAB platform to evaluate the effectiveness of the DG-AKU algorithm. The detailed simulation parameter settings are presented in Table 2. It is worth noting that the evaluation in this work is primarily based on simulation using synthetic parameters, which is consistent with many existing studies on theoretical security modeling. However, we acknowledge that real-world validation is essential for assessing deployment feasibility in practical ICV

environments. In particular, the lack of publicly available datasets that capture realistic attack traces for chosen-ciphertext attacks poses a challenge for empirical validation. In future work, the proposed framework can be integrated with real vehicular mobility datasets and more realistic communication models to improve external validity. Furthermore, prototype-level implementation and evaluation on edge computing platforms will be considered to assess computational overhead, communication latency, and system scalability in real deployments. The benchmark schemes are described as follows:

- Adaptive risk-sensing strategy (ARSS) [25]. This algorithm introduces the concept of continuous adaptive risk and trust assessment, in which security policies are dynamically adjusted by monitoring environmental risk indicators in real time.
- RL-based intelligent security (RL-IS) [26]. This algorithm proposes a risk-aware reinforcement learning framework, in which optimal defense strategies are learned through interactions between the agent and the environment.
- Static Key Update Strategy. This baseline adopts a fixed key update frequency that remains constant over time, without adapting to the evolving attack dynamics. It serves as a representative non-adaptive defense mechanism for comparison.
- Statistical Validation. This baseline evaluates the performance using simulated statistical patterns, providing a reference for assessing the significance and stability of the proposed method under stochastic variations.

Table 2: Parameter setting.

Parameters	Value
$\omega_1, \omega_2, \delta, \theta$	$(0,1)$
$\partial_1, \partial_2, \alpha_1, \alpha_2$	$[1,10]$
C_1, C_2, C_3, γ	$(0,10]$
g_2	0.6
g_1	0.8

Fig. 4 illustrates the evolution of the optimal key update frequency $f^*_{upd}(t)$ under the proposed DG-AKU framework and baseline methods. DG-AKU achieves superior performance due to the global optimization capability of the differential game model, exhibiting a smooth and rapid convergence to the Nash equilibrium. In contrast, RL-IS is affected by the exploration-exploitation trade-off, leading to initial stochastic fluctuations and convergence to a suboptimal local equilibrium. The ARSS mechanism, relying on threshold-based feedback, suffers from hysteresis and sensing noise, resulting in delayed adaptation and lower steady-state performance. These results demonstrate that DG-AKU outperforms baseline methods in convergence speed, stability, and optimality. The static key update strategy maintains a constant update frequency regardless of the system state, resulting in a lack of adaptability and inferior performance under dynamic attack conditions. Furthermore, the statistical validation confirms that the performance improvements achieved by DG-AKU over all baseline methods are statistically significant.

Fig. 5 illustrates the evolution of the optimal attack frequency. The DG-AKU strategy exhibits a smooth sigmoid trajectory and converges to the global Nash equilibrium in coordination with the defense strategy. Notably, the steady-state attack intensity remains below the corresponding defense level, indicating that the proposed mechanism leverages cost-benefit asymmetry to suppress rational attack escalation. In contrast, RL-IS shows stochastic fluctuations due to trial-and-error learning and converges to a suboptimal local equilibrium. Similarly, ARSS exhibits reactive oscillations and hysteresis, leading to inferior steady-state

performance. These results demonstrate that DG-AKU effectively reduces the attacker's incentive through game-theoretic interaction. In addition, the static key update baseline leads to a higher steady-state attack intensity, as the lack of adaptive defense allows the attacker to gradually escalate its strategy over time. The statistical validation baseline exhibits moderate and stable attack behavior with limited fluctuations, further confirming that the proposed DG-AKU framework more effectively suppresses the attacker's incentive compared with all baseline methods.

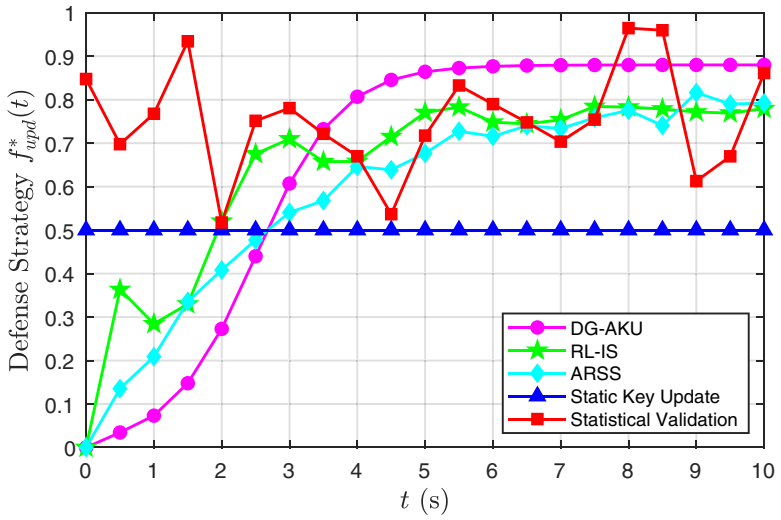

Figure 4: The defense strategy $f^*_{upd}(t)$ over time under different algorithms.

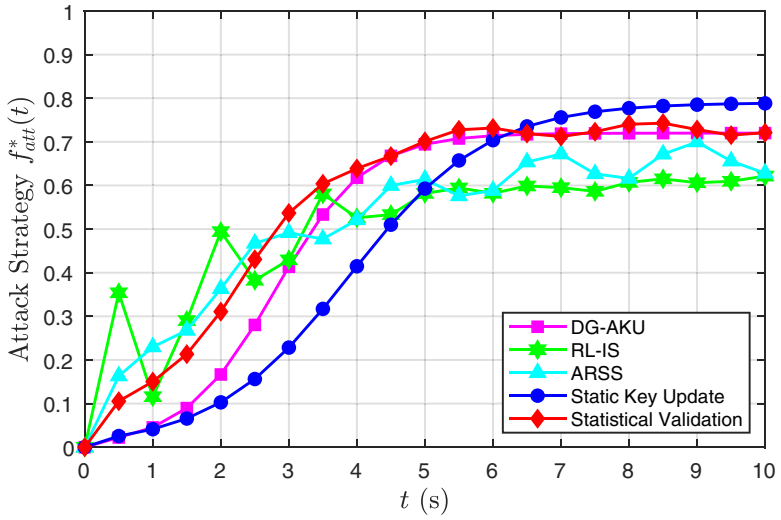

Figure 5: The attack strategy $f^*_{att}(t)$ over time under different algorithms.

Fig. 6 depicts the time-domain evolution of the normalized cumulative private-key leakage $x(t)$. DG-AKU demonstrates superior control performance, exhibiting a smooth monotonic decline that rapidly converges to the lowest level. This behavior is attributed to the predictive coordination of the differential game, which suppresses hysteresis and mitigates cumulative leakage. In contrast, ARSS shows a pronounced transient overshoot due to sensing delays inherent in threshold-based mechanisms, leading to initial

leakage accumulation. RL-IS exhibits persistent fluctuations driven by the exploration–exploitation trade-off, preventing stable convergence. These results highlight the robustness of DG-AKU in minimizing both transient and steady-state leakage.

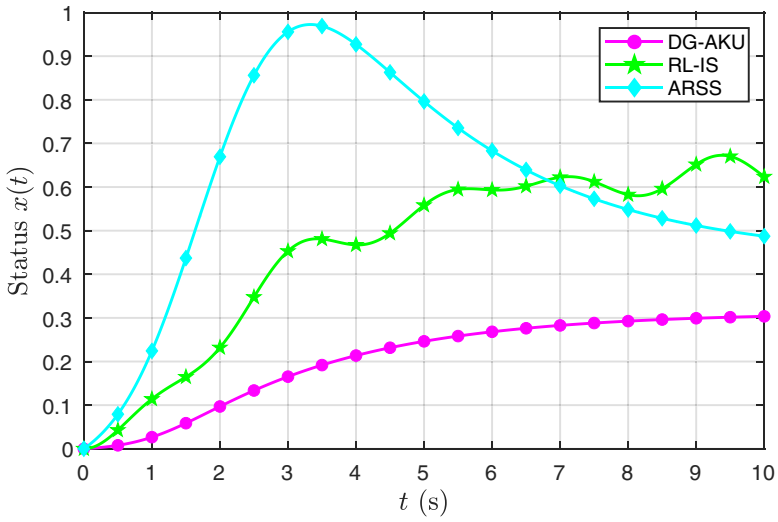

Figure 6: The status $x(t)$ over time under different algorithms.

Fig. 7 illustrates the sensitivity of the optimal defense strategy $f^*_{upd}(t)$ to the payoff discount factor α_2. In the low-discount regime (α_2 = 2.0), the strategy converges to a near-saturation level due to the high marginal value of future payoffs. In contrast, under a high discount factor (α_2 = 9.5), the perceived security benefit is significantly reduced, making high-frequency updates economically inefficient. Consequently, the system converges to a more conservative equilibrium that balances security gains with operational costs.

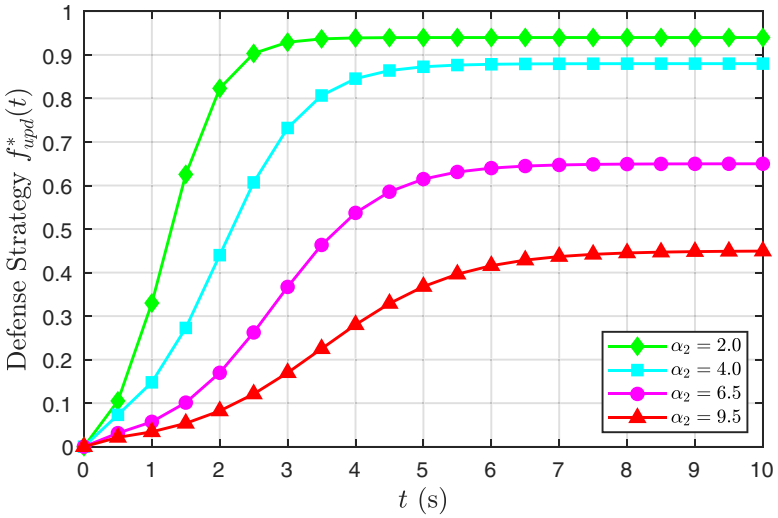

Figure 7: The defense strategy $f^*_{upd}(t)$ over time with different α_2.

Fig. 8 presents the curves of the defense strategy $f^*_{upd}(t)$ over time under different unit costs C_2. The evolution trajectories exhibit a strictly monotonic inverse relationship between the cost coefficient and the

equilibrium intensity of the control variable. In the low-cost regime ($C_2 = 0.5$), the strategy exhibits a quasi-step response characteristic, rapidly converging to a saturation level within the initial phase. Theoretically, negligible marginal costs trigger a Hamiltonian boundary solution, compelling the strategy to saturate at full capacity. In the high-cost domain ($C_2 = 9.0$), the optimal control trajectory is substantially suppressed. Prohibitive costs constrain the control strategy, inducing activation latency and amplitude attenuation. Consequently, the equilibrium defense frequency exhibits a monotonic inverse relationship with the cost parameter, indicating the model's capability for adaptive cost-aware regulation.

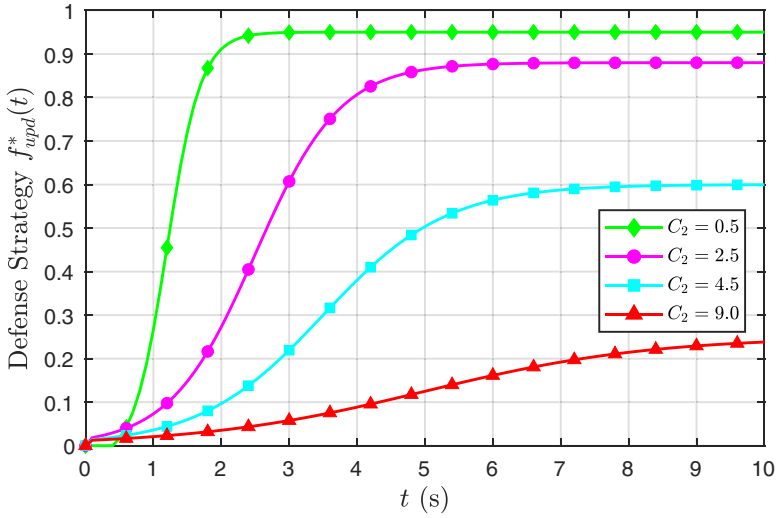

Figure 8: The defense strategy $f^*_{upd}(t)$ over time with different C_2.

Subsequently, we conduct a sensitivity analysis on the asymptotic behavior of the optimal defense strategy $f^*_{upd}(t)$. As evidenced by the temporal evolution trajectories, the system effectively converges to a stable Nash equilibrium at $t = 8$. Thus, we analyze how the steady-state value varies with C_2 and γ under different discount factors while fixing $t = 8$.

Fig. 9 illustrates the steady-state equilibrium of the defense strategy $f^*_{upd}(t)$ as a function of the unit cost C_2, under different discount factors $\alpha_2 \in \{2.0, 4.0, 6.5, 9.5\}$. The results show a monotonic inverse relationship between cost and defense intensity, with the decay rate governed by α_2. In the low-discount regime ($\alpha_2 = 2.0$), the strategy maintains a high equilibrium level over a wide cost range, indicating that the relatively high value of future payoffs offsets operational costs. In contrast, under a high discount factor ($\alpha_2 = 9.5$), defense intensity declines rapidly as cost increases, reflecting reduced marginal utility of defense and a narrower feasible region for active strategies.

Fig. 10 elucidates the steady-state equilibrium of the defense strategy $f^*_{upd}(t)$ as a function of the cost discount factor γ, parameterized by the game discount rate $r \in \{0.05, 0.15, 0.30, 0.50\}$. Specifically, in the low-discount regime ($r = 0.05$), the defense strategy rapidly converges to the saturation equilibrium, due to the sustained valuation of future utility. Conversely, in the high-discount domain ($r = 0.50$), the attenuation of future payoffs constrains the defense intensity. As a result, the strategy converges to a suppressed steady-state level even as the cost discount factor increases. These observations indicate that while γ influences the magnitude of the response, r determines the sensitivity and the asymptotic upper bound of the optimal strategy.

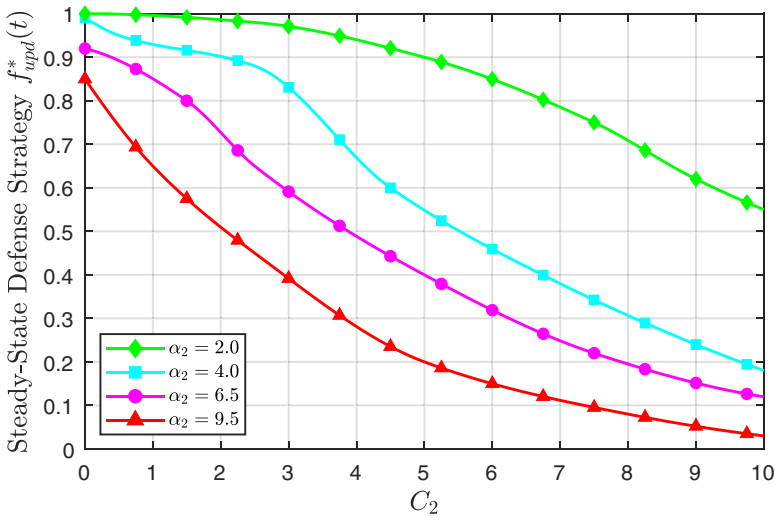

Figure 9: The variation of $f^*_{upd}(t)$ steady-state value with C_2 when $t = 8$.

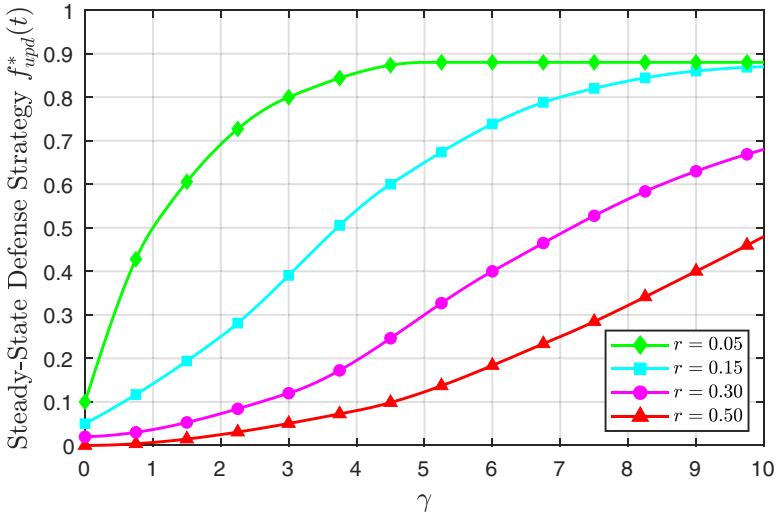

Figure 10: The variation of $f^*_{upd}(t)$ steady-state value with γ when $t = 8$.

Fig. 11 illustrates the discrete-time evolution of the optimal defense strategy $f^*_{upd}(t)$ under different private key leakage risks θ. The results reveal a monotonic positive relationship between θ and defense intensity across all time steps. In the high-risk regime ($\theta = 0.8$), the strategy rapidly converges to a saturation level, reflecting strong defense to preserve forward secrecy. In contrast, under low risk ($\theta = 0.2$), the strategy remains at a low level, indicating that the marginal benefit of frequent updates does not justify the associated cost. This demonstrates the model's capability for risk-aware adaptive regulation.

Fig. 12 illustrates the discrete-time evolution of the optimal defense strategy $f^*_{upd}(t)$ under varying update efficiency factors ω_2. The results show a monotonic positive relationship between ω_2 and defense intensity across all time steps. The strategy exhibits nonlinear saturation behavior: when $\omega_2 \in [0.2, 0.4]$, $f^*_{upd}(t)$ increases rapidly, indicating high sensitivity to efficiency gains; when $\omega_2 \in [0.6, 0.8]$, the growth rate diminishes as the strategy approaches its equilibrium bound. This pattern reflects adaptive modulation

of defense intensity with respect to ω_2, leading to maximization of the Hamiltonian within the feasible control set.

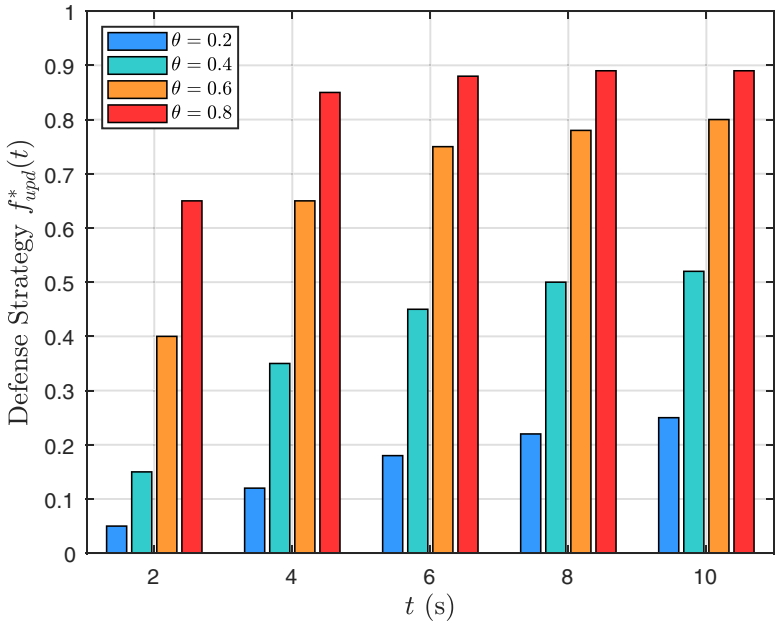

Figure 11: The variation of $f^*_{upd}(t)$ with t under different θ.

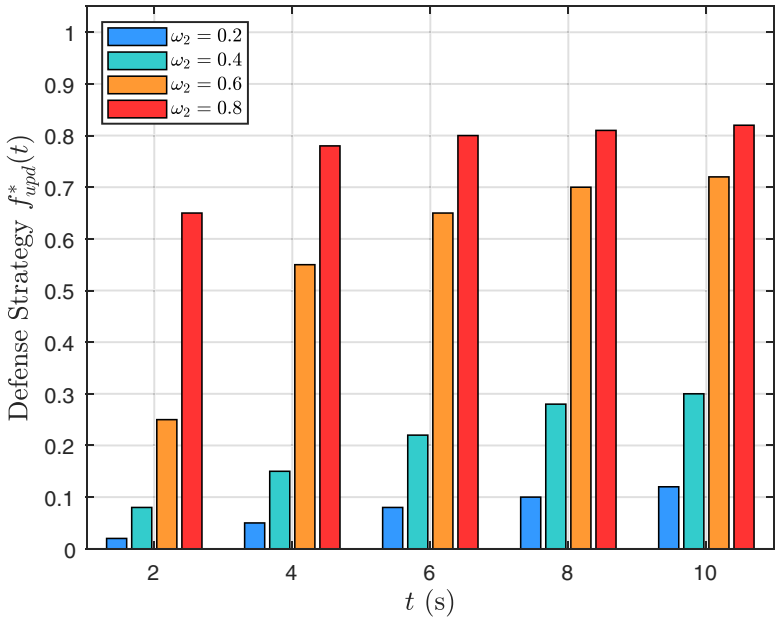

Figure 12: The variation of $f^*_{upd}(t)$ with t under different ω_2.

6 Conclusions

This paper addresses long-term privacy leakage risks of ICV location data at the SP side, focusing on the mismatch between static key management and dynamic CCA. We propose a differential game-based

adaptive key update mechanism that adjusts the Paillier private key update frequency under time-varying attacks, ensuring forward secrecy while minimizing system overhead. Specifically, cumulative private-key information leakage is modeled as the core state variable in a continuous-time stochastic differential game capturing attacker-defender interactions. By solving the HJB equations, the optimal defense strategy under the Nash equilibrium is derived. Simulation results demonstrate that the proposed mechanism effectively maximizes defense utility while suppressing attacker information accumulation. Furthermore, sensitivity analyses on key parameters-including the cost discount factor, game discount rate, privacy leakage risk, and efficiency impact factor-validate the rationality and robustness of the model, providing theoretical support for data security defense in ICV systems.

In future work, the proposed framework can be extended to account for more realistic system conditions, such as imperfect attack detection and discrete-time dynamics. Moreover, practical deployment in ICV environments requires further consideration of computational constraints, communication overhead, and scalability across large-scale vehicular networks. Future research may also explore multi-agent extensions, heterogeneous vehicle behaviors, and more sophisticated adversarial models to further enhance the robustness and applicability of the proposed approach.

Acknowledgement: None.

Funding Statement: This work was supported in part by the Key Program of the National Natural Science Foundation of China under Grant 62436004; and in part by the General Program under Grant 62372317.

Author Contributions: Conceptualization, Lei Wang, Hongji Luo, Jianwei An, Haitao Xu, Xianwei Zhou; methodology, Yong Heng, Jingnan Tang, Haitao Xu; writing—original draft preparation, Lei Wang, Xiaochuan Ju, Jianwei An; writing—review and editing, Lei Wang, Hongji Luo, Yong Heng, Jingnan Tang, Xiaochuan Ju, Jianwei An, Haitao Xu, and Xianwei Zhou. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Qiu M, Yu W, Wang L, Zhang B, Zhao H. A regenerative braking control strategy for ICVs considering the coupling effect of driving conditions and driving styles. IEEE Trans Veh Technol. 2023 Feb;72(6):7195–210. doi:10.1109/TVT.2023.3242729.
2. Tang J, Zhu H, Lu R, Lin X, Li H, Wang F. DLP: achieve customizable location privacy with deceptive dummy techniques in LBS applications. IEEE Internet Things J. 2021 Sep;9(9):6969–84. doi:10.1109/JIOT.2021.3115849.
3. Sun G, Liao D, Li H, Yu H, Chang V. L2P2: a location-label based approach for privacy preserving in LBS. Future Gener Comput Syst. 2017 Sep;74(5):375–84. doi:10.1016/j.future.2016.08.023.
4. Ullah I, Ali Shah M, Khan A, Guizani M. Location privacy schemes in vehicular networks: taxonomy, comparative analysis, design challenges, and future opportunities. ACM Comput Surv. 2025 Feb;57(6):1–44. doi:10.1145/3711681.
5. Zhang H, Cao L, Kumar N, Zhang J, Zhang P, Wang J. An improved DDPG-based privacy sensitive level protection computation offloading method in mobile edge computing. Future Gener Comput Syst. 2024 Oct;159(5):522–32. doi:10.1016/j.future.2024.05.018.
6. Srijayanthi S, Sethukarasi T. Design of privacy preserving model based on clustering involved anonymization along with feature selection. Comput Secur. 2023 Mar;126(1):103027. doi:10.1016/j.cose.2022.103027.
7. Jiang S, Yang H, Xie Q, Ma C, Wang S, Liu Z, et al. Towards compute-efficient Byzantine-robust federated learning with fully homomorphic encryption. Nat Mach Intell. 2025 Sep;7(10):1657–68. doi:10.1038/s42256-025-01107-6.

8. Bojjagani S, Reddy YP, Anuradha T, Rao PV, Reddy BR, Khan MK. Secure authentication and key management protocol for deployment of Internet of Vehicles (IoV) concerning intelligent transport systems. IEEE Trans Intell Transp Syst. 2022 Sep;23(12):24698–713. doi:10.1109/TITS.2022.3207593.
9. Li Z, Shi G. A CCA-secure puncturable attribute-based proxy re-encryption scheme. IEEE Internet Things J. 2025 Aug;12(22):47679–90. doi:10.1109/JIOT.2025.3604341.
10. Kitagawa F, Matsuda T, Tanaka K. CCA security and trapdoor functions via key-dependent-message security. J Cryptol. 2022 Feb;35(2):9. doi:10.1007/s00145-022-09420-8.
11. Liu X, Zhang H, Dong S, Zhang Y. Network defense decision-making based on a stochastic game system and a deep recurrent Q-network. Comput Secur. 2021 Dec;111(15):102480. doi:10.1016/j.cose.2021.102480.
12. Jiang N, Zhai Y, Wang Y, Yin X, Yang S, Xu P. Location privacy protection for the internet of things with edge computing based on clustering K-anonymity. Sensors. 2024 Sep;24(18):6153. doi:10.3390/s24186153.
13. Khodaei M, Papadimitratos P. Cooperative location privacy in vehicular networks: why simple mix zones are not enough. IEEE Internet Things J. 2020 Dec;8(10):7985–8004. doi:10.1109/JIOT.2020.3043640.
14. Masood S, Hassan MU, Tsai PW, Chen J. DLLPM: dual-layer location privacy matching in V2V energy trading. J Syst Archit. 2025 Oct;167(11):103507. doi:10.1016/j.sysarc.2025.103507.
15. Zhao Y, Zhao J, Yang M, Wang T, Wang N, Lyu L, et al. Local differential privacy-based federated learning for internet of things. IEEE Internet Things J. 2020 Nov;8(11):8836–53. doi:10.1109/JIOT.2020.3037194.
16. Jiang B, Li J, Yue G, Song H. Differential privacy for industrial internet of things: opportunities, applications, and challenges. IEEE Internet Things J. 2021 Feb;8(13):10430–51. doi:10.1109/JIOT.2021.3057419.
17. Liu Z, Cao Z, Dong X, Zhao X, Liu T, Bao H, et al. EPMDA-FED: efficient and privacy-preserving multidimensional data aggregation scheme with fast error detection in smart grid. IEEE Internet Things J. 2021 Sep;9(9):6922–33. doi:10.1109/JIOT.2021.3113519.
18. Liu Y, James J, Kang J, Niyato D, Zhang S. Privacy-preserving traffic flow prediction: a federated learning approach. IEEE Internet Things J. 2020 Apr;7(8):7751–63. doi:10.1109/JIOT.2020.2991401.
19. Mohammadali A, Haghighi MS. A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid. IEEE Trans Smart Grid. 2021 Jan;12(6):5212–20. doi:10.1109/TSG.2021.3049222.
20. Liu W, You L, Shao Y, Shen X, Hu G, Shi J, et al. From accuracy to approximation: a survey on approximate homomorphic encryption and its applications. Comput Sci Rev. 2025 Feb;55(11):100689. doi:10.1016/j.cosrev.2024.100689.
21. Mohammed A, Razzak R, Rahouti M, Yazdinejad A, Parizi RM, Qolomany B, et al. Safeguarding connected autonomous vehicle communication: protocols, intra-and inter-vehicular attacks and defenses. Comput Secur. 2025 Apr;151(4):104352. doi:10.1016/j.cose.2025.104352.
22. Zhang Z, Huang W, Huang Y, Liao Y, Wu C, Zhou S. An attribute-based pre-authenticated secure communication protocol enabling key protection and credential online-upgrading for 5G NR V2X. IEEE Trans Intell Transp Syst. 2025 Apr;26(8):11325–41. doi:10.1109/TITS.2025.3558978.
23. Khan AA, Kumar V, Ahmad M, Rana S. LLAKAF: lightweight authentication and key agreement framework for smart grid network. J Syst Archit. 2021 Jun;116(2):102053. doi:10.1016/j.sysarc.2021.102053.
24. Calvo M, Beltrán M. A model for risk-based adaptive security controls. Comput Secur. 2022 Apr;115(2):102612. doi:10.1016/j.cose.2022.102612.
25. Guo H, Wu X, Liu J, Mao B, Chen X. Adaptive and reliable location privacy risk sensing in Internet of Vehicles. IEEE Trans Intell Transp Syst. 2024 May;25(9):12696–708. doi:10.1109/TITS.2024.3384464.
26. Lu X, Xiao L, Xiao Y, Wang W, Qi N, Wang Q. Risk-aware federated reinforcement learning-based secure IoV communications. IEEE Trans Mob Comput. 2024 Aug;23(12):14656–71. doi:10.1109/TMC.2024.3447019.
27. Zhang L, Zhu T, Xiong P, Zhou W, Yu PS. More than privacy: adopting differential privacy in game-theoretic mechanism design. ACM Comput Surv (CSUR). 2021 Jul;54(7):1–37. doi:10.1145/3460771.
28. Saiyed MF, Al-Anbagi I. A game theoretic model for strategic defence selection against DDoS attacks in IoT networks. IEEE Trans Netw Serv Manag. 2025 Jul;22(5):4509–24. doi:10.1109/TNSM.2025.3589901.

29. Guo C, Wang S, Yu K, Zhu Y, Tao X. A differential game method against DDoS attacks in IoT Botnets: holistic and dynamic perspectives. IEEE Internet Things J. 2025 Feb;12(12):19414–27. doi:10.1109/JIOT.2025.3541852.
30. Wang Y, Lang P, Tian D, Zhou J, Duan X, Cao Y, et al. A game-based computation offloading method in vehicular multiaccess edge computing networks. IEEE Internet Things J. 2020 Feb;7(6):4987–96. doi:10.1109/JIOT.2020.2972061.
31. Wang Y, Nedić A. Differentially private distributed algorithms for aggregative games with guaranteed convergence. IEEE Trans Automat Contr. 2024 Jan;69(8):5168–83. doi:10.1109/TAC.2024.3351068.
32. Zhang Y, Tian K, Lu Y, Liu F, Li C, Gong Z, et al. Reparable threshold Paillier encryption scheme for federated learning. Soft Comput. 2025 May;29(7):1–6. doi:10.1007/s00500-025-10640-w.
33. Singh S, Reddy P. Dynamic network analysis of a target defense differential game with limited observations. arXiv 2021. IEEE Trans Control Netw Syst. 2023 Aug;10:308–20. doi:10.1109/TCNS.2022.3203358.
34. Miao L, Li S. A differential game-theoretic approach for the intrusion prevention systems and attackers in wireless networks. Wirel Pers Commun. 2018 Jun;103(3):1993–2003. doi:10.1007/s11277-018-5892-1.