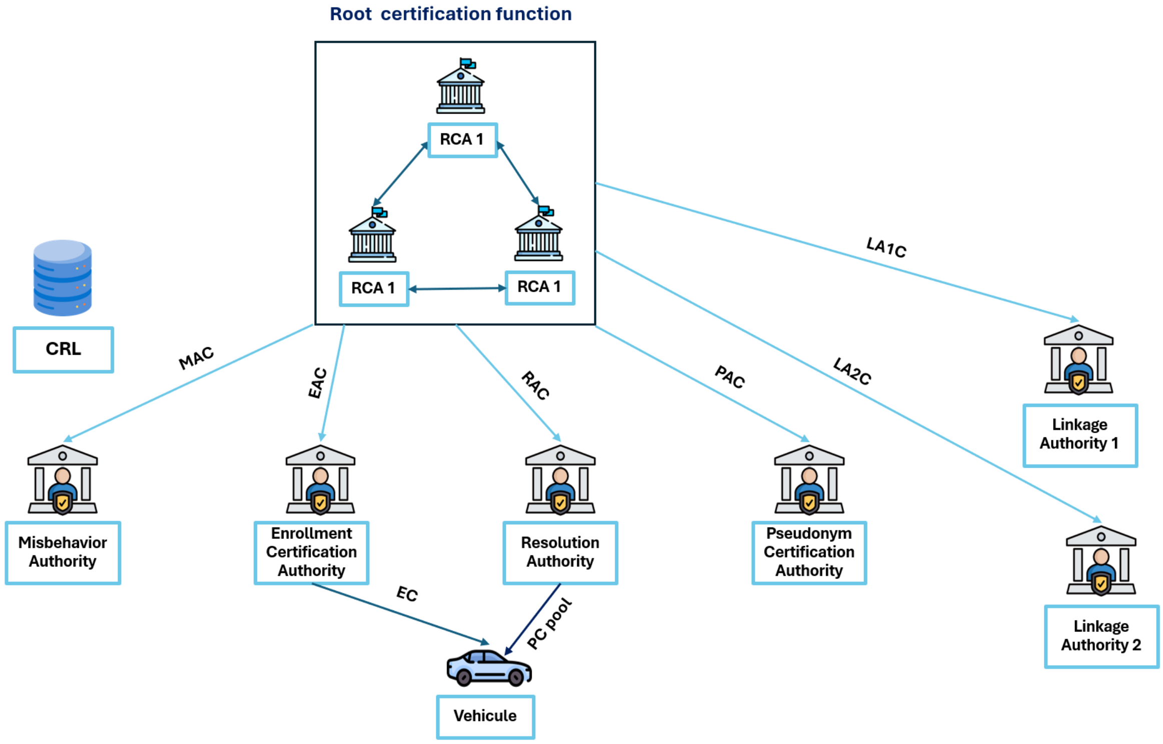
Proposition

Architecture



Root Certification Authority (RCA 1-3): The Root Certification Authority (RCA) acts as the primary trust anchor in a PKI, and deploying multiple RCAs is recommended for several key reasons; Deploying multiple RCAs enhances scalability and interoperability by simplifying PKI expansion and merging, thereby avoiding extensive re-issuance of certificates and updates to the CRL. It maintains existing hierarchies and dependencies. Additionally, it boosts resiliency; if an RCA is compromised, only its hierarchy is affected, reducing the overall impact and limiting the need to replace all certificates.

Enrolment Certification Authority (ECA): The Enrollment Certification Authority (ECA) is a vital component of the PKI infrastructure, acting as the entry point for each ITSS and functioning as a Registration Authority during the Initialization/Bootstrap phase. It issues Enrollment Certificates (ECs) to C-ITS devices, enabling them to authenticate with other authorities and request services. Additionally, the ECA assigns unique canonical identifiers to each device for consistent identification throughout their lifecycle. The ECA also collaborates with the Pseudonym Certification Authority (PCA) in providing pseudonym certificates.

Pseudonym Certificate Authority (PCA 1-3): The Pseudonym Certification Authority (PCAx) provides pseudonym credentials to ensure secure V2X communications. Although decentralization is recommended, we have opted for a single PCA to simplify collaboration and management. The PCA issues pseudonym certificates to ITS stations already enrolled with the ECA and works with it to verify the identity of ITSSs requesting new pseudonym certificates. Additionally, the PCA collaborates with the Misbehavior Authority, to identify misbehaving ITSS.

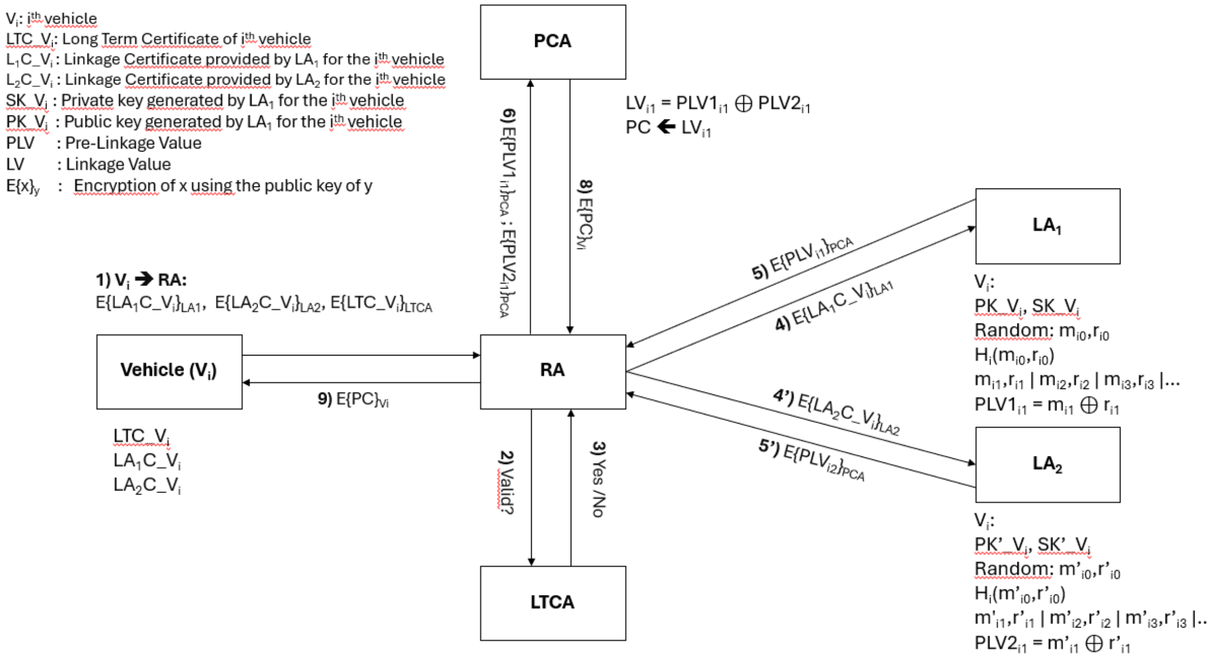
Misbehavior Authority (MA): The Misbehavior Authority (MA) plays a crucial role in securing Cooperative Intelligent Transport Systems (C-ITS) networks by excluding misbehaving stations from the trust domain, ensuring their messages are ignored. The MA receives misbehavior reports from stations and analyzes them to determine if revocation is necessary. If misbehavior is detected, the MA works with the PCA to identify the ITSS and creates an entry in the Certificate Revocation List (CRL). The MA then communicates the identity of the misbehaving ITSS to the ECA for inclusion in the CRL.

Setup: system parameters

Enrollment certificate provisioning:

During the enrollment phase, a device with a valid canonical ID contacts the Enrollment Certificate function, which randomly selects an Enrollment Certification Authority (ECAx) to issue the Enrollment Certificate (EC) to that user. The Enrollment Certification Authority x generates two additive and multiplicative groups $G1$ and $G2$, respectively, with the same prime order q. The generators of $G1$ and $G2$ are P and g, respectively. Let Zq be a finite field of order q. The master secret key sk is per vehicle chosen randomly from Zq. Then, the corresponding public key PK is derived, and the system's public parameters $\{G1, G2, P, g, q, Hc\}$ are published while keeping sk secret. The process involves the ITS-S sending an Enrollment Request message to the EA. Upon receiving the request, the EA processes it and issues the EC, SK, and corresponding public key if the request meets the necessary criteria. The selected ECA x saves the corresponding Enrollment Certificate, canonical ID, secret key (SK), public key (PK), and public parameters (q, g, and P) in its database. Additionally, the EA issues two other certificates related to linkage authorities LA1 and LA2 (LA1C_Vi and LA2C_Vi).

Pseudonym certificate provisioning:


V_i: i^{th} vehicle
LTC_V_i: Long Term Certificate of i^{th} vehicle
L_1C_V_i : Linkage Certificate provided by LA_1 for the i^{th} vehicle
L_2C_V_i : Linkage Certificate provided by LA_2 for the i^{th} vehicle
SK_V_i : Private key generated by LA_1 for the i^{th} vehicle
PK_V_i : Public key generated by LA_1 for the i^{th} vehicle
PLV : Pre-Linkage Value
LV : Linkage Value
$E\{x\}_y$: Encryption of x using the public key of y
PCA
RA
LTCA
Vehicle (V_i)
LA_1
LA_2
1) V_i → RA:
$E\{LA_1C\_V_i\}_{LA1}$, $E\{LA_2C\_V_i\}_{LA2}$, $E\{LTC\_V_i\}_{LTCA}$
9) $E\{PC\}_{Vi}$
2) Valid?
3) Yes /No
6) $E\{PLV1_{i1}\}_{PCA}$; $E\{PLV2_{i1}\}_{PCA}$
8) $E\{PC\}_{Vi}$
$LV_{i1} = PLV1_{i1} \oplus PLV2_{i1}$
PC ← LV_{i1}
5) $E\{PLV_{i1}\}_{PCA}$
4) $E\{LA_1C\_V_i\}_{LA1}$
4') $E\{LA_2C\_V_i\}_{LA2}$
5') $E\{PLV_{i2}\}_{PCA}$
LTC_V_i
LA_1C_V_i
LA_2C_V_i
V_i:
PK_V_i, SK_V_i
Random: m_{i0},r_{i0}
$H_i(m_{i0},r_{i0})$
m_{i1},r_{i1} | m_{i2},r_{i2} | m_{i3},r_{i3} |…
$PLV1_{i1} = m_{i1} \oplus r_{i1}$
V_i:
PK'_V_i, SK'_V_i
Random: m'_{i0},r'_{i0}
$H_i(m'_{i0},r'_{i0})$
m'_{i1},r'_{i1} | m'_{i2},r'_{i2} | m'_{i3},r'_{i3} |..
$PLV2_{i1} = m'_{i1} \oplus r'_{i1}$

The Intelligent Transport System Station (ITS-S) must be enrolled beforehand to request pseudonym certificates from the Pseudonym Certification Authority (PCA). The ITS-S possesses pseudonym certificates allowing it to send signed messages to other ITS-S without revealing its canonical identity or enrollment credentials. It can obtain or update its pseudonym certificates by sending Pseudonym Requests. Once all pseudonym certificates are used, the ITS-S reverts to the initial enrollment state. The process ensures pseudonymity and is divided into several phases:

1. Pseudonym Certificate Request

The vehicle Vi sends a Pseudonym Certificate Request to the Registration Authority (RA). The request contains The Long-Term Certificate ($LTCVi$), Linkage Certificates ($LA1CV$i), and ($LA2CVi$) encrypted using the public keys of LA1 and LA2 respectively. The Long-Term Certificate is encrypted using the public key of the LTCA. The Linkage Certificates are used as identifiers by the Linkage Authorities (LA1 and LA2) to determine which hash belongs to the vehicle without knowing the real identity of the vehicle.

2. Validation

The RA validates the request by checking the certificates with the Long-Term Certificate Authority (LTCA) to ensure the authenticity of the vehicle.

3. Forwarding Certificates

If the certificates are valid, the RA forwards the Linkage Certificates to Linkage Authority 1 (LA1) and Linkage Authority 2 (LA2) respectively.

4. Generation of Linkage Values

4.1. LA1:

Generates a random value $mi1{,}0$mi1,0 and a randomness factor $ri1{,}0$r i1,0 from Zq. Computes the chameleon hash

$Hi1=Hc(ri1{,}0\ ;\ mi1{,}0)=g\hat{}(mi1{,}0+ski1\cdot ri1{,}0)=g\hat{}(mi1{,}0)\cdot g\hat{}(ski1\cdot ri1{,}0)$. Generates the Pre-Linkage Value ($PLVi1$) as $mi1\bigoplus ri1$

Encrypts the Pre-Linkage Value with the public key of the PCA and sends it to the RA.

4.2. LA2:

Generates a random value $mi1{,}0$mi1,0 and a randomness factor $ri2{,}0$; r i2,0 from Zq. Computes the chameleon hash

$Hi2=Hc(ri2{,}0\ ;\ mi2{,}0)=g\hat{}(mi2{,}0+ski2\cdot ri1{,}0)=g\hat{}(mi2{,}0)\cdot g\hat{}(ski2\cdot ri1{,}0)$.. Generates the Pre-Linkage Value ($PLVi2$) as $mi2\bigoplus ri2$

Encrypts the Pre-Linkage Value with the public key of the PCA and sends it to the RA.

5. Calculation of Linkage Value

The PCA calculates the Linkage Value

$LVi1$ by combining the Pre-Linkage Values received from LA1 and LA2:

$LVi1=PLVi1\bigoplus PLVi2$

Then sends the Pseudonym Certificate (PC) request to the RA.

6. Pseudonym Certificate Issuance

The PCA issues the Pseudonym Certificate (PC) based on the received request and the linkage value $LVi1$. The pseudonym certificate includes the Linkage Value, ensuring that the vehicle has a pool of pseudonyms for secure communication.

Misbehavior and Revocation:

The Misbehavior Authority (MA) receives Misbehavior Reports (MRs) generated by ITS stations. Upon receiving an MR, the MA evaluates the provided evidence to determine whether misbehavior has occurred. This assessment involves analyzing the observations, received messages, and proofs contained within the report. Based on this analysis, the MA decides whether the reported behavior constitutes misbehavior according to established criteria and system policies.

If misbehavior is confirmed, the MA initiates appropriate response and remediation actions to address the issue and protect the system. The MA identifies the involved pseudonyms (PR) and communicates with the Pseudonym Certification Authority (PCA). The PCA retrieves the Pre-Linkage Values (PLV1 and PLV2) associated with the reported pseudonyms and sends these values back to the respective Linkage Authorities (LA1 and LA2), requesting all related Pre-Linkage Values (PLV) they have issued. LA1 and LA2 respond by providing all related PLVs. The PCA then calculates the Linkage Values (LV) using the received PLVs and includes these LVs in the Certificate Revocation List (CRL) along with the corresponding hash.

When a vehicle receives a message intended for another vehicle, it processes the message by verifying the pseudonym. The vehicle searches for the Linkage Value (LV) in the CRL to ensure the pseudonym has not been revoked. If the LV is found in the CRL, the vehicle discards the message, ensuring that only valid and non-revoked pseudonyms are accepted. This process maintains the integrity and security of communications within the system by ensuring that any misuse of pseudonyms is promptly identified and addressed.

Procedure 1: Key and Parameters Generating

System Setup Function: The system setup function, performed by the enrollment authority before the enrollment of vehicles, generates two groups: an additive group $G1$ and a multiplicative group $G2$, both with the same prime order q. The generators of $G1$ and $G2$ are P and g, respectively. Let Zq be a finite field of order q. The public parameters $\{G1, G2, P, g, q, Hc\}$ are computed and saved. These system parameters are stored correctly to meet the required cryptographic properties and are made available for subsequent cryptographic operations.

Output: public parameters $\{G1, G2, P, g, q, Hc\}$

Key Generation Function: The key generation process begins when the enrollment authority receives a request from a vehicle to generate the enrollment certificate. The vehicle provides its canonical ID to prove its identity. For each vehicle, the enrollment authority generates a unique identifier and the corresponding keys using the Discrete Logarithm Problem (DLP)(generated this way). This process begins by defining the security parameter λ to set the bit length for the prime p. A random prime p of bit length λ is generated, and q is computed as $(p - 1)/2$. A master secret key sk is then chosen randomly from Zq. The corresponding public key PK is derived using the formula PK = g^sk mod p. The keys are securely saved by the enrollment authority, ensuring proper documentation and security.

Input: λ, canonical ID

Function: KeyGen(λ) → (sk, pk, {G_1, G_2, P, g, q})

Output: ID, sk, pk

Function 2: Chameleon Hash Calculation and Storage Algorithm

The process unfolds as follows: Initially, during the enrollment phase, the pseudonym authority provides the enrollment certificate and requests the enrollment authority to generate a unique identifier. This identifier is used to associate the generated hash values with a specific entry in the key storage file. The function readKeysFromFile(filePath, identifier) then retrieves the values of p, q, g, pk, and sk from the file. These parameters are crucial for subsequent chameleon hash computations. The file is scanned to match the provided identifier, extracting the associated cryptographic values. Next, using the randgen function, random values $r1$ and $\mathrm{msg}1$ are generated within the range defined by q. The chameleonHash function computes the chameleon hash based on these parameters and random values. This computation involves hashing e as e = $H(message||r1)$ using the SHA-256 hash function.

Subsequently, the computed hash is inserted back into the file under the corresponding identifier using the insertHash1(filePath, identifier, hash1) function. This operation includes reading the file contents, locating the identifier, and appending the computed hash value.

Input: ID, message, r, sk, pk

Function: ChameleonHash(p, q, g, hk, message, r, sk) → hash

Output: hash

Function 3: Generating Collision and Pseudonym Pool Creation

Function: generateCollision(hk, tk, p, q, g, msg1, msg2, r1, s1, r2, s2)

Pseudonym i = (msgi ,r2i➙ generatePseudonym(Identifier,i))

The pseudonym generation process within the chameleon hash scheme is structured to ensure robust cryptographic security and operational efficiency. Initially, the algorithm prompts for a unique identifier, establishing a dedicated directory to house generated pseudonyms associated with this identifier. Essential cryptographic parameters, namely p, q, g, hk, and tk, are retrieved from a predefined file. These parameters serve as foundational elements for subsequent operations. Beginning with the initialization of random values msg1, r1, and s1, the algorithm computes their chameleon hash (hash1) using the **SHA-256 cryptographic** hash function. Following this, collisions are systematically generated based on a user-specified count. **Each collision involves the random generation of msg2, followed by the computation of corresponding values r2 and s2.** These values are computed to maintain collision resistance properties within the defined cryptographic framework.

Security analysis

The enrollment authority is trusted and operated by the government, the PCA is a trusted but curious authority these two cannot be compromised. Vehicles are considered honest and malicious at the same time.

In our threat model, we assume that one or more attackers, with access only to pseudonymous data (LVi), are attempting to obtain unauthorized access to a vehicle's long-term data. Alternatively, the attacker may seek to acquire pseudonym-linking information to monitor a specific vehicle within the VANET.

Protocol proprieties

1. Intractability

Intractability ensures that an attacker cannot feasibly compute the secret keys or derive pseudonyms without access to the private information and trapdoors held by the authorities.

How it is preserved:

Enrollment Phase: During enrollment, each vehicle receives an Enrollment Certificate (EC), including a secret key sk and a public key pk. The public parameters $\{G1, G2, P, g, q, Hc\}$ are published, but the secret key sk is kept confidential. The difficulty of deriving sk from pk relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is computationally intractable.

Pseudonym Certificate Issuance: When pseudonym certificates are issued, the PCA calculates the Linkage Value (LV) using the Pre-Linkage Values (PLV1 and PLV2) provided by LA1 and LA2. Using chameleon hashes with trapdoors ensures that the PCA can generate valid pseudonym certificates without exposing the trapdoor or secret keys, thus preserving intractability. Furthermore, no authority (PCA, LA1, or LA2) can identify the user or the related pseudonyms. This guarantees that even if an outsider takes control of one of these authorities, they cannot identify the user or the associated pseudonyms.

2. Unlikability

Unlikability ensures that an observer cannot link multiple pseudonyms to the same vehicle.

How it is preserved:

Pseudonym Requests and Issuance: Each pseudonym request generates new ECC key pairs, ensuring that pseudonyms are independent of each other.

The chameleon hash function, Hc, provides collision resistance and the ability to produce different hashes for different pseudonyms, even if they correspond to the same vehicle.

PLV and LV Usage: By using PLVs from two independent linkage authorities (LA1 and LA2) and computing the LV as $LVi1=PLV1i1\bigoplus PLV2i1$, the protocol ensures that each pseudonym's linkage value is unique and unlikable to previous or future pseudonyms.

3. Pseudonymity of a Vehicle

Pseudonymity ensures that the real identity of a vehicle cannot be determined from its pseudonyms.

How it is preserved:

Public Key Infrastructure: The public and private keys used in pseudonyms are generated and managed by the PCA and LAs without revealing the vehicle's canonical identity. The encryption of requests and responses ensures that only authorized entities can access the relevant keys and pseudonyms.

Chameleon Hash Function: The use of chameleon hashes allows the PCA to issue pseudonyms without knowing the underlying identity, as the hashes can be computed using the trapdoor held by the LAs. This preserves the vehicle's pseudonymity by preventing any direct linkage between pseudonyms and the vehicle's identity.

Authority Isolation: Since no single authority (PCA, LA1, or LA2) has complete information about the user or the issued pseudonyms, even if one authority is compromised, the attacker cannot deduce the identity of the user or link the pseudonyms to the user.

4. Revocation:

Revocation ensures that misbehaving vehicles can be identified, and their pseudonyms can be invalidated.

How it is preserved:

Misbehavior Detection: The MA evaluates Misbehavior Reports and identifies the pseudonyms involved. The PCA retrieves the corresponding PLVs and calculates the LVs, which are then included in the CRL.

CRL Distribution: The CRL is distributed to all vehicles, allowing them to check received messages against the list of revoked pseudonyms. This ensures that messages from misbehaving vehicles are discarded, maintaining the security and integrity of the network.

How these Properties are Preserved:

From Outside Attackers:

- Encryption and Secure Communication: All communications involving certificate requests and responses are encrypted, preventing external attackers from intercepting or deciphering messages.
- Randomized and Frequent Changes: The use of randomized key generation and frequent pseudonym changes ensure that attackers cannot build a reliable profile of a vehicle.

From Internal Authorities:

- Role Separation and Minimal Information Sharing: By compartmentalizing the roles of the RA, LTCA, PCA, LA1, LA2 and MA, the system ensures that no single authority has access to both the real identity and the pseudonym of the vehicle simultaneously.
- Audit and Monitoring: Regular audits and strict protocols ensure that internal authorities do not misuse their roles to de-anonymize vehicles without due cause.

Cryptography proprieties:

1. Unforgeability:

Ensures that pseudonym certificates and associated messages cannot be forged or impersonated by an attacker.

Preservation Mechanism:

- Digital Signatures: Pseudonym certificates and messages are digitally signed by the issuing authority (PCA). This signature ensures that any modification or forgery attempt can be detected since the digital signature will no longer match.
- Chameleon Hashing: Used in the generation of Pre-Linkage Values by Linkage Authorities (LA1 and LA2). Since chameleon hashes allow for a controlled way to change the hash value, if necessary, but require the knowledge of a secret to generate a valid hash, any attempt to forge or tamper with these values can be detected.

2. Indistinguishability:

Ensures that pseudonym certificates issued to different vehicles are indistinguishable from each other, preventing attackers from linking them to specific vehicles.

Preservation Mechanism:

- Randomized Values: The process involves generating random values (e.g., mi1,0 and mi2,0) and randomness factors (ri1,0 and ri2,0). This randomness, combined with chameleon hashing, ensures that pseudonym certificates for different vehicles appear indistinguishable, preventing attackers from correlating certificates to specific vehicles.
- Butterfly Key Expansion: The use of butterfly key expansion in generating unique signing keys adds another layer of obfuscation, making each pseudonym certificate unique and difficult to trace back to the vehicle.

3. Confidentiality:

Ensures that messages and data are only accessible to authorized parties, preventing unauthorized access.

Preservation Mechanism:

- Encryption: Pseudonym certificates and pre-linkage values are encrypted using public keys of relevant authorities (e.g., PCA). This encryption protects the data during transmission and ensures that only authorized entities can decrypt and access the information.
- Symmetric and Asymmetric Cryptography: The use of both symmetric (for fast encryption/decryption) and asymmetric cryptography (for secure key exchange and encryption) ensures that data remains confidential throughout its lifecycle, from request to issuance.

4. Integrity:

Ensures that the data within pseudonym certificates and messages has not been altered or tampered with.

Preservation Mechanism:

- Digital Signatures and Hash Functions: Digital signatures are used to verify the authenticity and integrity of pseudonym certificates. Any modification to the data would result in a mismatch of the signature. Additionally, hash functions are employed to ensure that data integrity is maintained.
- Chameleon Hashing: Ensures the integrity of the pre-linkage values by providing a hash function that can verify the correctness of the linkage values. Tampering with these values will lead to incorrect hash results, which can be detected.