Turk J Elec Eng & Comp Sci
() : –

doi:10.3906/elk-

Privacy-Preserving and Verifiable Product Rating Aggregation in E-Commerce Using Threshold Homomorphic Encryption with Distributed Key Generation

Received: .202 • **Accepted/Published Online:** .202 • **Final Version:** ..202

1. Background

We first introduce the cryptographic primitives that form the basis of our privacy-preserving and verifiable rating-aggregation protocol. In contrast to conventional centralized architectures, our design relies on threshold homomorphic encryption, distributed key generation, and verifiable secure computation to simultaneously guarantee confidentiality, correctness, and transparency.

1.1. Threshold Homomorphic Encryption

Let $N = pq$. denote an RSA modulus where p and q are large safe primes. We adopt an additive homomorphic encryption scheme such as Paillier or CKKS [16], which enables integer addition to be performed directly over ciphertexts. A homomorphic public key pk_{HE} is published to all clients in the system. The corresponding private decryption key sk_{HE} is never constructed in full. Instead, the secret key is shared among n aggregation servers by means of a t-out-of-n threshold cryptosystem, derived from Shamir's secret sharing. Each server S_{i} holds a private share sk_{i}, and decryption is only possible when a quorum of at least t servers jointly participate in the threshold decryption algorithm. This approach eliminates any single point of failure and prevents a malicious server from decrypting user ratings individually.

1.2. Distributed Key Generation (DKG)

To avoid dependence on a trusted dealer, we integrate a distributed key generation protocol such as Pedersen DKG [14] or multi-round DKG In these protocols, each server independently selects a random polynomial of degree $t-1$ and distributes verifiable Shamir shares to the other servers using verifiable secret sharing (VSS). Once the protocol terminates: all servers collectively derive a unique public key pk_{HE}; each server retains exactly one valid and publicly verifiable share of the secret key. Since no individual server learns the complete secret key, the system achieves robustness against collusion of up to $t-1$ corrupted servers.

1.3. Privacy-Preserving Aggregation Flow

Following the establishment of the threshold key pair, the secure aggregation of product ratings proceeds through the following steps: 1. Rating Submission: A client c computes an encrypted rating $C = \mathrm{Enc}_{pk_{\mathrm{HE}}}(r_{\mathrm{c}})$ $r_{\mathrm{c}} \in \{1, 2, 3, 4, 5\}$

To prevent malformed inputs, the client attaches a non-interactive zero-knowledge (NIZK) range proof demonstrating that the encrypted value lies within the valid domain. 2. Validation and Collection: Aggregation servers verify the submitted range proof and store the encrypted rating if the proof is valid. No server gains access to the plaintext rating at this stage. 3. Homomorphic Aggregation: Using the additive homomorphism of the encryption scheme, servers compute the encrypted sum and the encrypted count of all received ratings:

$$C_{\mathrm{sum}} = \prod_{\mathrm{i}} C_{\mathrm{i}}, \qquad C_{\mathrm{count}} = \mathrm{Enc}_{pk_{\mathrm{HE}}}(m)$$

where m is the total number of ratings. These operations require no interaction with users and do not reveal any individual input.

1.4. Threshold Decryption

Once aggregation is complete, at least ttt servers jointly produce partial decryptions of the ciphertexts. Each partial decryption is accompanied by a verifiable proof showing that it was computed honestly. The final plaintext values are reconstructed only when enough valid partial decryptions have been collected.

1.5. Public Verifiability

Anyone can verify the correctness of the final aggregation by checking the NIZK proofs, the partial decryption proofs, and the consistency of the reconstructed results. This ensures transparency without sacrificing user privacy. This secure computation pipeline allows our protocol to preserve the confidentiality of individual ratings while enabling publicly auditable computation of global statistics over large-scale e-commerce datasets.