MATSUURA LAB.

Cryptography and Information Security

Department of Informatics and Electronics

Department of Information and Communication Engineering,
Graduate School of Information Science and Technology

Information Security

http://kmlab.iis.u-tokyo.ac.jp/

Matsuura Lab is aiming at making a technical contribution to the construction of systems where people can easily and securely exchange information. The research areas of Matsuura Lab includes cryptography, information security and network protocols.

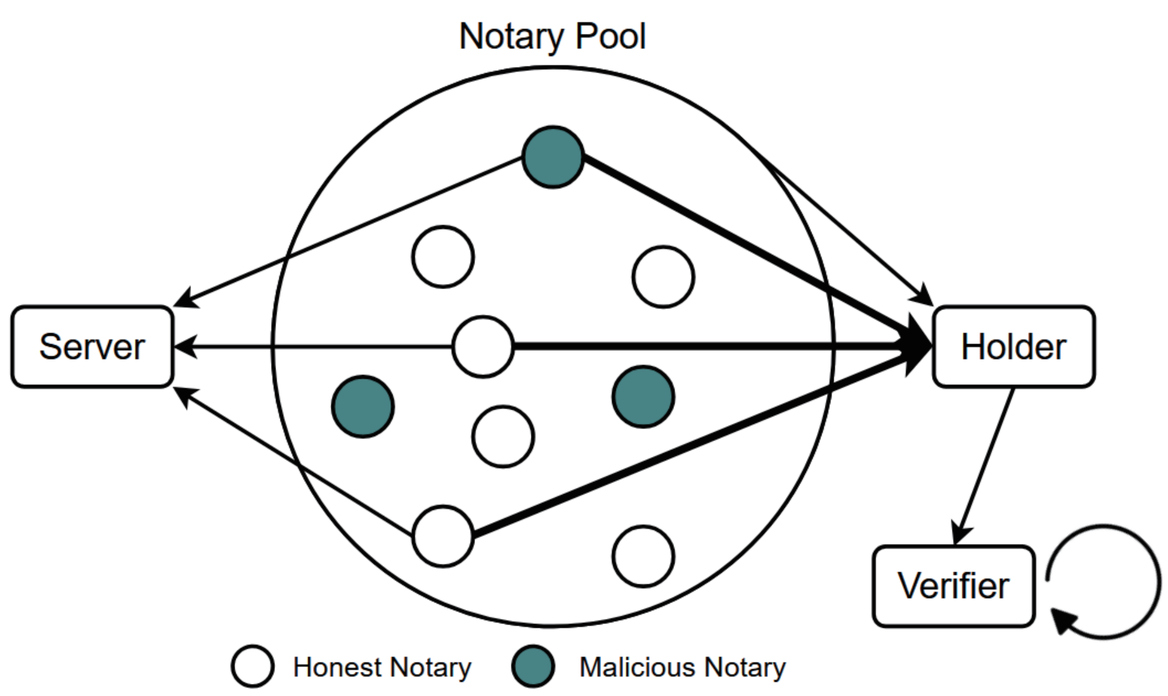
Turning Web Information into "Trustworthy Proof"

- From TLS to Verifiable Credentials—Distributed Notaries with Incentives -

Screenshots of web pages are often used in expense claims and verification procedures. But screenshots are easy to edit, and it is hard for recipients to mechanically confirm that the information truly came from the claimed site. Many web services do not provide built-in provenance proofs. This research explores a system that records web information not as a screenshot, but as "trustworthy proof" that can later be verified by a third party.

Proposed Mechanism

A notary relays TLS communication between a user and a web server and, without seeing the plaintext, signs the communication record to attest that it was not altered after retrieval. The signed record can be stored and presented as Verifiable Credentials (VCs), without requiring server-side changes.
To avoid reliance on a single notary, we use multiple notaries and consider incentive mechanisms (e.g., collateral and forfeiture) so that cheating is unprofitable, potentially achieving the same assurance with fewer participants and lower cost.



Applications

In cases such as expense reimbursement from card statements, enrollment verification via a university website, or proof of bank balance, users can submit a verifiable proof instead of a screenshot.
Recipients can use the attached signatures to mechanically verify the source and detect tampering, and wider adoption could support standardized and automated verification.