T-PKI: a Cryptographic Scheme based on Public Key Infrastructure with Many Unlinkable Public Keys

by

Art Sedighi

Major: Computer Engineering

Department: Electrical and Computer Engineering

Program of Study Committee:

Thomas Daniels, Major Professor

Doug Jacobson, Major Professor

Berk Gulmezoglu

Goce Trajcevski

Kevin Scheibe

Iowa State University

Ames, Iowa

2023

Copyright © Art Sedighi, 2023. All rights reserved.

This page intentionally left blank

ABSTRACT

This body of work introduces the Transactional Public Key Infrastructure (T-PKI) where a single private key can generate a potentially infinite number of public keys. Each public key is disposable after use and, thus, unlinkable to the originator. Each new public key generated from the same private key can be used for a new transaction or a message in a P2P system, and the same private key can be used to decrypt any message encrypted with the public key.

Public Key Infrastructure (PKI), an integral part of peer-to-peer communication, exposes the public key from the participants as part of the protocol handshake. In cases where anonymity is desired, the public key could become an attack vector which could expose the recipient of a message. One or few messages do not leak much information, but a collection of messages could reveal a pattern where anonymity could be pierced and participants exposed. The desire for anonymity has led to several privacy preservation techniques, where a scheme is desired to reduce the digital footprint to eliminate the ability to utilize social engineering to deduce private information about the participants.

The current state of literature around anonymity for transactions is focused on blockchain anonymity concerns, with the lack of anonymity of Bitcoin being the key concern. The Bitcoin blockchain is fully transparent and can be mined for patterns, usage, and transactions. The transparency of the Bitcoin blockchain aides the solving of the double-spending issue. However, the research in this area has demonstrated how the Bitcoin blockchain can be extracted for information. Even though it is Bitcoin’s pseudonym that is saved on the blockchain, it is possible to combine social engineering along with data engineering to break the anonymity barrier and determine the participants of a transaction.

Another area under consideration would be peer-to-peer communication where public key is used to encrypt messages sent amongst the participants. In such cases, an eavesdropper can monitor the public keys being shared, and deduce information about the recipient of the message. Peer-to-peer communication in the digital world of electronic agreements is also considered where an interested party (e.g. purchaser of goods) is sending messages as part of an agreement as part of a transaction. These transactions could represent purchases from online merchants, peer-to-peer systems such as cryptocurrencies, or auction sites. A single transaction may not leak much information about the interested parties, but a collection could leak information about the participants.

T-PKI prevents systematic collection of public information leaked about the participants of peer-to-peer communication which could be used to deanonymize the participants. In an earlier work, T-PKI was considered for other uses such as anonymizing the attestation sent by a Trusted Computing Module (TPM) to a verifier in Internet of Things (IoT) devices where privacy is desired. The programming interface to T-PKI is that of the Learning with Errors (LWE) lattice-based cryptographic scheme, and that allows easy integration and development of the protocol to systems currently utilizing LWE.

The T-PKI simulator (tSim), a python-based simulation environment for security protocols, is used to simulate the four stages of keypair generation, public key generation, encryption and decryption for T-PKI, LWE and RSA protocols under various security levels. T-PKI performs as well as LWE for different bit-security levels and performs better than RSA in 192- and 256-bit security levels. LWE and RSA, however, are not able to generate a new public key without generating the entire keypair.