非対称計算機資源環境における認証システム

概要

認証のための通信手順において証明者（センサー、タグ等）の計算資源（メモリー、処理能力）が検証者の計算資源よりも乏しい場合、十分軽量でないところが課題であった。
本発明は非対称計算機資源環境における認証の際に、証明者は検証者から届いたチャレンジを２つの雑音と共有情報を加えレスポンスを生成し、検証者が作成したローカルレスポンスと作られたレスポンスを比較することで認証を行う技術である。
この技術により計算資源が乏しいデバイスの認証を安全に低動作コストで行うことができる。

特徴

・２つの認証プロトコルを用いたことにより片側の動作コスト低減と安全性を両立（公開鍵ではなく共通鍵系の軽量暗号技術）
・以下の２つの組み合わせで安全性を担保
  ・LPN問題、ランダムセレクション問題
  ・ストリーム暗号、ランダムセレクション、暗号文のランダム化

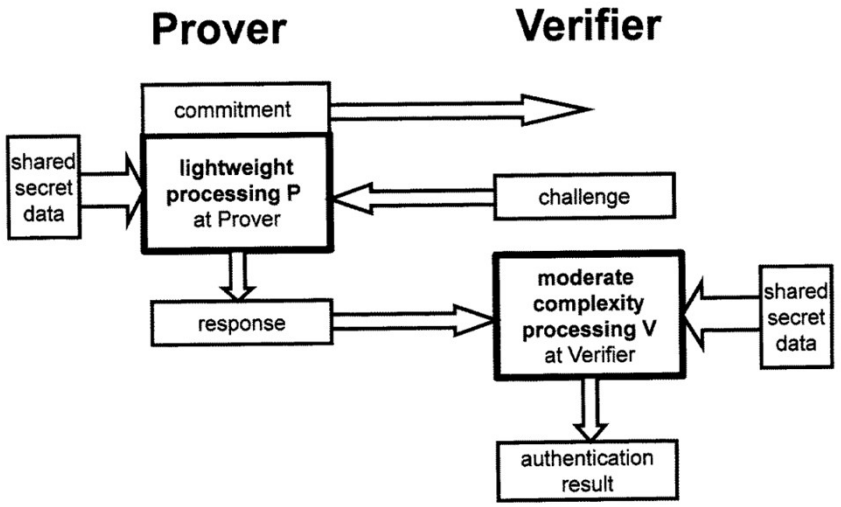

図１：認証フレームワーク

発明者

生産技術研究所　松浦幹太教授　他
http://kmlab.iis.u-tokyo.ac.jp/index_j.html
（発明者への直接のお問い合わせはご遠慮ください）

特許情報

特許成立（特許第6602210号）
https://www.j-platpat.inpit.go.jp/c1800/PU/JP-6602210/D0DCFEB7DE71E85B071E55387AC186ADEF8AA96A5452384B5353754B3FE2E5EF/15/ja

お問合せ先

株式会社 東京大学TLO　浅見 唯葉
TEL：03-6706-1629
Email：asami@todaitlo.jp
HP：https://todaitlo.com/

非対称計算機資源環境における認証システム

プロトコル１

・LPN問題、ランダムセレクション問題

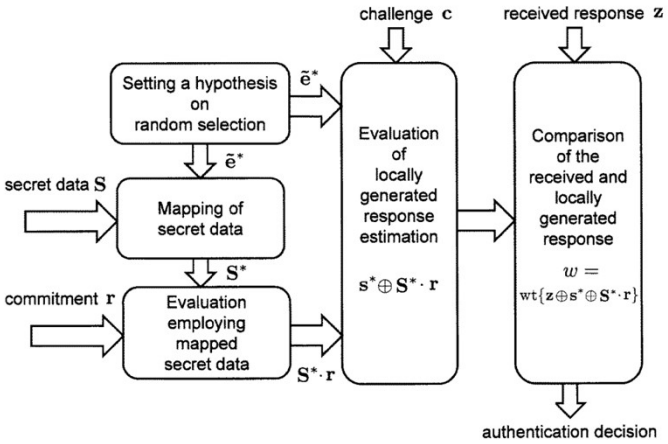

図２：プロトコル１における証明者における処理

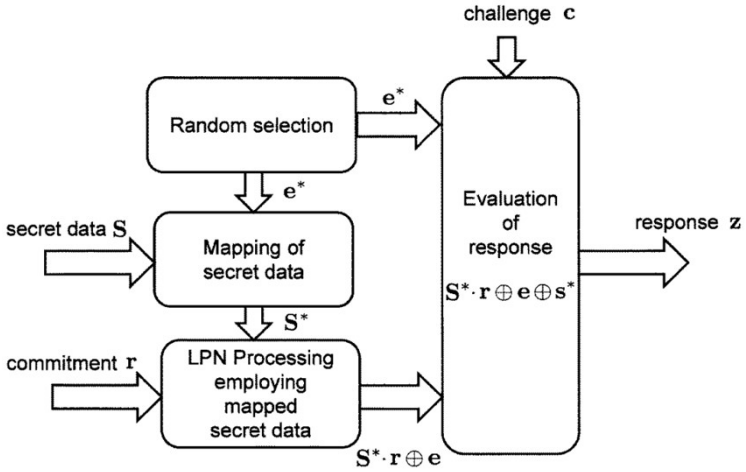

図３：プロトコル１における検証者における処理

プロトコル2

・ストリーム暗号、ランダムセレクション、暗号文のランダム化

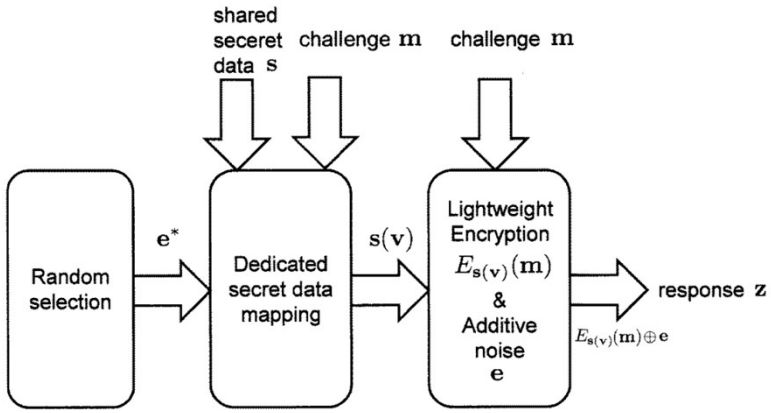

図２：プロトコル２における証明者における処理

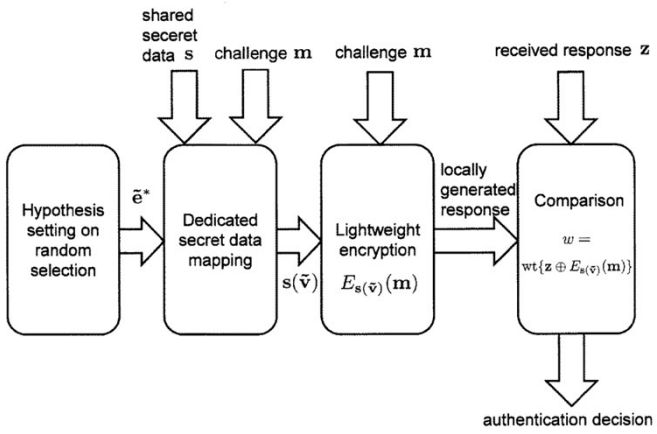

図３：プロトコル２における検証者における処理