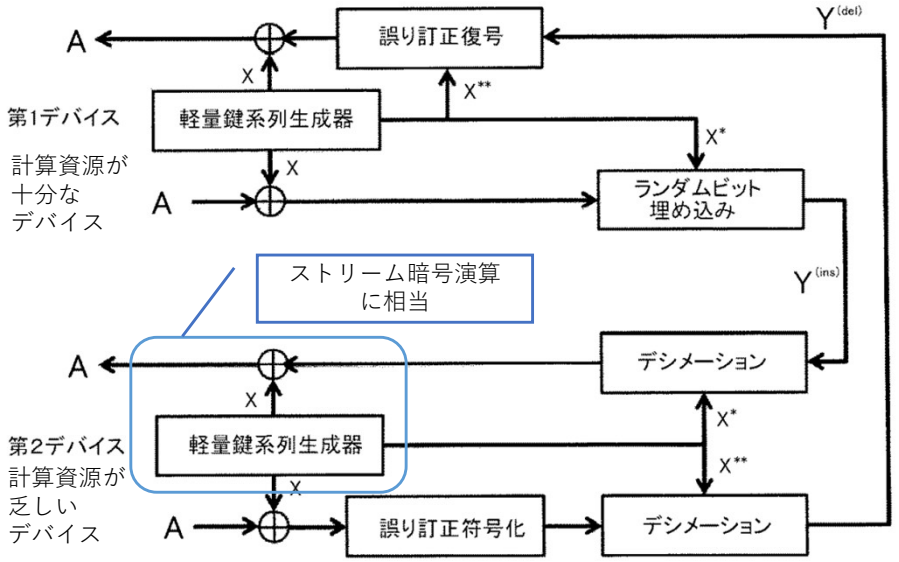
非対称計算機資源環境における暗号通信

概要

計算資源（メモリー、処理能力）を節約して計算機が暗号通信を行う際に使用するストリーム暗号は計算資源が乏しいデバイス（センサー、タグ等）からすると処理が重すぎるところが課題であった。本発明は暗号通信が非対称計算機資源環境で行われる場合に、デシメーションと埋め込み処理のコスト差を利用して、安全性を担保したまま片方のデバイスの計算量を軽くする暗号通信技術である。この技術により計算資源が乏しいデバイスが暗号化、複合化のどちらを行う場合であっても安全性と低動作コストが実現した。

特徴

・デシメーションと埋め込みのコスト差により、片側の動作コスト低減と安全性を両立した暗号
・ランダムな雑音の挿入、信号の欠落により符号理論により暗号の安全性を担保（公開鍵ではなく共通鍵系の軽量暗号技術）



発明者

生産技術研究所　松浦幹太教授
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6667174号）
https://www.j-platpat.inpit.go.jp/c1800/PU/JP-6667174/01FC7B340810081F052DB3F2548A30C37E7C90E04FA4BC55C36F66AA153CC4ED/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暗号通信

第１デバイス：計算資源が十分なデバイス

第２デバイス：計算資源が乏しいデバイス

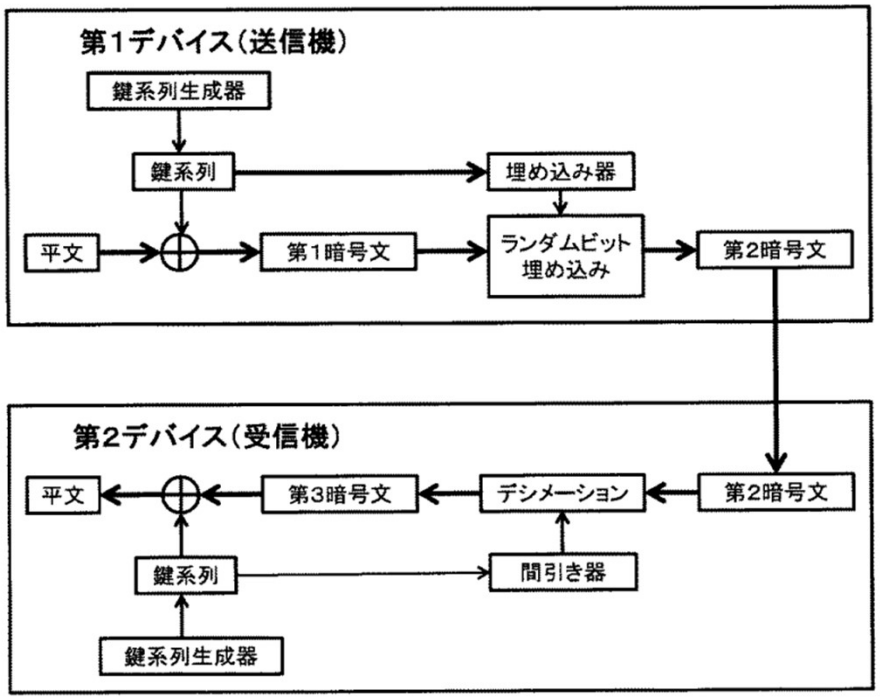


図２：計算資源が乏しいデバイスからの送信

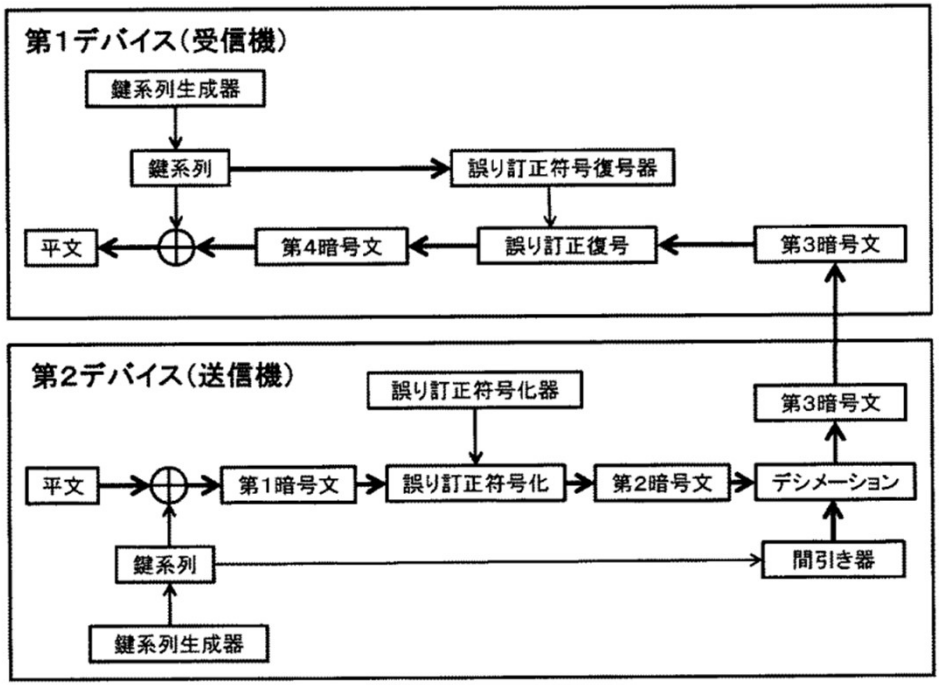


図３：計算資源が乏しいデバイスでの受信