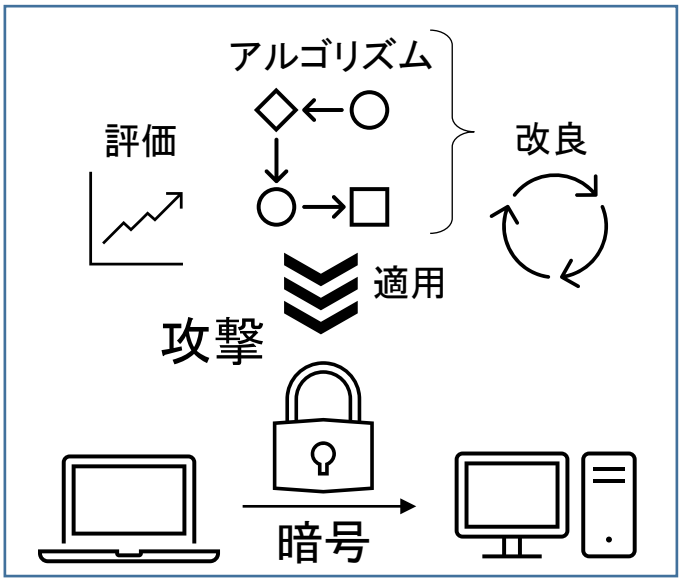
情報

中村　周平　研究室

代数的アルゴリズムを利用した暗号の安全性解析

公開鍵暗号は通信の安全性を数学問題の困難性に帰着することを目指した技術です。本研究室では特に、安全性の根拠となる数学問題を連立代数方程式問題に帰着させる攻撃の効率性について調べ、この攻撃からの暗号の安全性解析を行います。具体的には、求解手法の改良やアルゴリズムの計算量見積もりを行います。



キーワード　連立代数方程式問題、暗号理論

分　　野　情報科学