平成29年度 情報工学コース卒業研究報告要旨

楫 研究室	氏　　名	柏 倉　祐 吉
卒業研究題目	Winternitz ワンタイム署名の改良とその評価	

現在広く使われている電子署名は, 素因数分解等の数論的な問題を現実的な時間で解くことの難しさが安全性の根拠となっている. 一方, 数論的な問題を効率よく解くことのできる量子コンピュータの実用化研究が急速に進んでおり, 今日広く使われている電子署名の多くは, 近い将来に無力化される可能性がある. そのため数論的な問題に依拠せず電子署名を実現する研究が展開されている. しかし鍵や署名が長くなったり, 必要な計算量が大きくなってしまうために, 電力消費の観点からバッテリ駆動の小型機器等での運用は困難であるものも多い.

暗号学的ハッシュ関数を利用した電子署名技術であるワンタイム署名 (OTS) は, 数論的な問題に依拠しない電子署名の実現方式の一つである. 運用に若干の制限はあるが, OTS を用いることにより, 比較的小さなオーバヘッドで量子コンピュータへの高い安全性を確保することができる. 本研究では, 代表的な OTS として知られる Winternitz OTS に改良を加え, 安全性を確保したまま署名長や計算量を削減する方式を提案する.

Winternitz OTS では, 複数のハッシュ連鎖を構成して鍵を生成し, 常に全ての連鎖を利用して署名を計算する. 提案手法では, それに加えて鍵生成時にハッシュ連鎖を余分に構成しておき, 全ての連鎖から鍵を生成するが, 署名作成時はメッセージ内容に応じて利用するハッシュ連鎖を選択し, 選ばれた一部の連鎖だけを用いて Winternitz OTS の署名作成手続きを実行する. 署名作成時にハッシュ連鎖の一部を選択するという手続きを経由することによって, 署名の値域は選択の組み合わせの総数倍に増加する. 結果として, 署名作成および検証における計算量や署名長に関わるパラメータの増加を抑えながら安全性を確保できる. 以上が本研究における基本的なアイデアである.

提案手法と Winternitz OTS の性能を詳細に比較したところ, 提案手法を用いることによって鍵長が長くなる可能性があるが, 署名のサイズの削減や署名作成および検証の計算量の削減効果が生じることが明らかになった. これらの結果より, 提案手法は, 量子コンピュータの出現に対しても安全であり, 小型機器等における実装にも有利であると結論付けることができる.