学位論文題目　実装を考慮した暗号解析手法に関する研究
取得年月　2009年3月　**学位種別**　博士（工学）　**大学**　筑波大学
氏　名　武仲 正彦（（株）富士通研究所 主任研究員）
推薦研究会　コンピュータセキュリティ
推薦文　本論文は，実装を中心として暗号技術のさまざまな課題を議論している幅の広い論文である．中でも，公開鍵の偽造問題に関する研究成果は重要で，公表されて社会的に大きなインパクトを与えた．したがって，その実用性を高く評価して，ここに推薦申し上げます．

近年，電子商取引やWebシステムを利用したサービスが盛んになっており，これら多くの通信が，最も重要な社会インフラの1つであるインターネットを経由して行われている．インターネット上のサービスでは，個人情報，契約情報，クレジットカード番号等の機密情報が第三者を経由して送信される．機密情報を安全に送信するためには，データの秘匿，認証，署名などを実現する暗号技術は必須である．

利用者にとって，暗号技術はさまざまな面から安全であることが期待される．それにはまず，暗号技術の仕様だけではなく，その実装までが安全である必要がある．仕様と実装の双方が安全でなければ，暗号技術の安全な利用を保証できない．また，各暗号技術は，暗号アルゴリズムそのものである暗号プリミティブと，それをどのように動作させるかを規定する暗号スキームにより構成される．そのため，暗号技術の安全な利用には，暗号プリミティブと暗号スキームの両面からも安全であることが求められる．暗号技術を安全に機能させるためには，これらあらゆる面からの安全性評価が必要である．

本論文では，暗号技術の仕様と実装の安全性評価に役立つ3つの暗号解析手法を提案し，暗号技術の実装の安全性評価の重要性について議論を行う．本論文の主な貢献は下記の4点である．(1) 暗号プリミティブの仕様に対する解析手法として，実験的な解析しか行われてこなかった共通鍵ブロック暗号RC6のχ^2攻撃についてのモデル化を実施し，RC6のχ^2攻撃に対する詳細なセキュリティ評価を実現．(2) 暗号プリミティブの実装の解析手法として，Address- bit DPAと呼ばれる解析手法を拡張し，Address-bit DPA対策の必要性が認識されていなかった公開鍵暗号プリミティブOK-ECCの実装解析が可能であることの提示．(3) 暗号スキームの実装に対する解析手法として，Bleichenbacher攻撃と呼ばれる署名偽造手法を拡張し，その拡張手法を効果的に適用することで，実運用されているタイムスタンプの偽造が可能であることの提示．(4) これら3つの解析による安全性評価を比較し，その社会的な影響を分析することで，実装を考慮した暗号解析の重要性を提示．

図-1

特に(3) Bleichenbacher攻撃署名偽造手法の拡張では，偽造が可能となる実装の可能性を示すだけではなく，**図-1**に示すように，実際に市販されている製品で偽造タイムスタンプが正しいと誤判定される脆弱性を指摘し，実社会に対し大きな影響を与えた．また，本脆弱性については，(独) 情報処理推進機構(IPA)に届け出を実施，開発会社との情報交換を行うことで，修正／アップデートに貢献した．

従来，暗号技術の安全な利用のために，暗号プリミティブの仕様解析が中心に行われてきた．しかし，本研究(3)で示した，実装の不具合を悪用する解析の研究はほとんど行われていない．一方で現在，バッファオーバフローやSQLインジェクションなど，アプリケーションの不具合を利用するシステムへの攻撃が多数発生し，社会問題となっている．そのため今後，本研究と同様，暗号スキームの実装の不具合を利用した攻撃が増加し，実装を考慮した暗号技術の解析が重要になると考えられる．

(平成22年3月10日受付)