組み込み機器は要注意！アルゴリズムだけじゃ安全じゃない!?

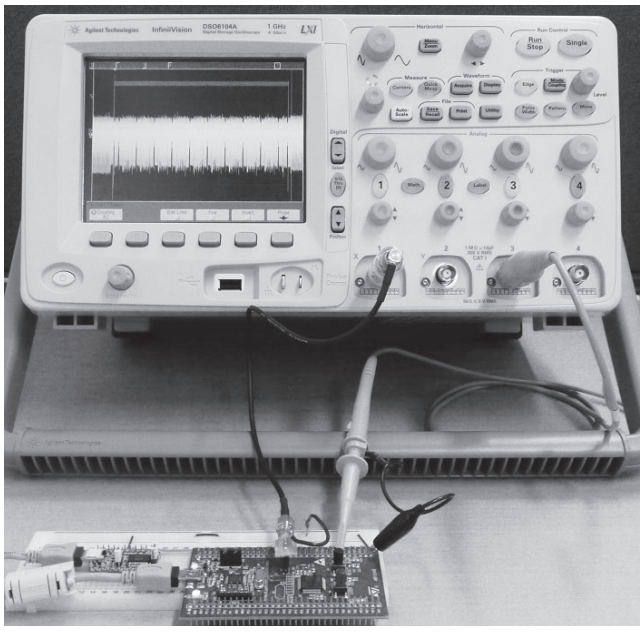
研究最先端！

マイコンの消費電力解析による暗号解読

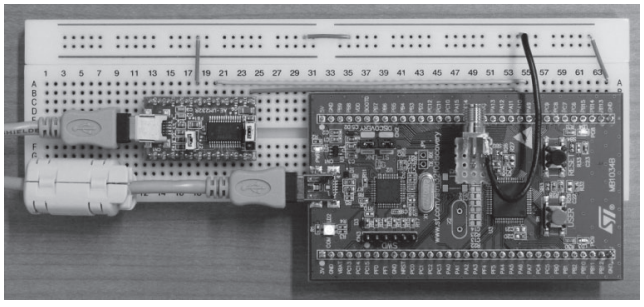
後編

128ビットAES暗号の解読実験とサイドチャネル攻撃対策

片下 敏宏，堀 洋平



（a）全体



（b）ホストPCとの通信用にUSB-シリアル変換モジュールを追加

写真1　実験のようす

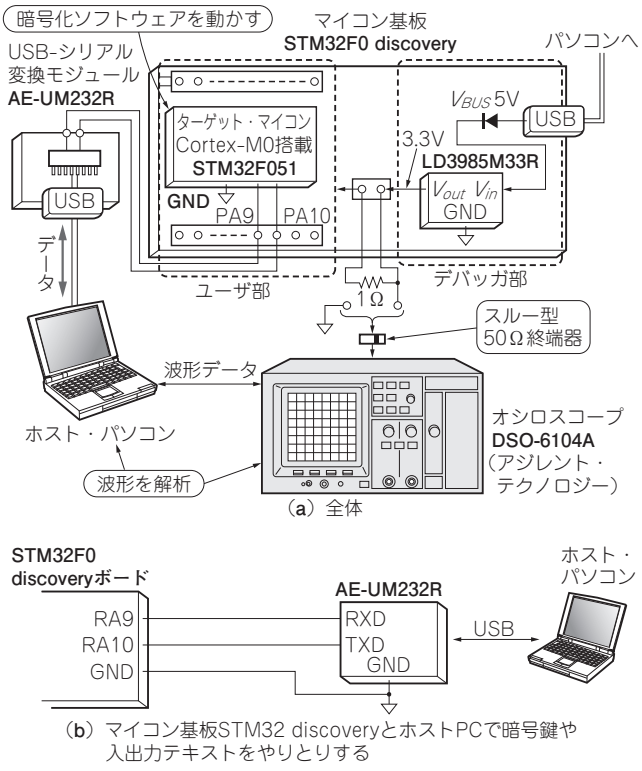


図1　消費電力解析による暗号解読を試す！実験の構成

Wi-Fiやキーレス・エントリ，ICカード，音楽・動画などディジタル・コンテンツの著作権保護など，マイコン/CPUで暗号化を使うことが増えてきました．各種制御システム，自動車，医療機器などでの利用も見込まれています．暗号には理論的な評価がなされた安全なアルゴリズムを用いますが，実はそれだけでは十分ではありません．

マイコン/CPUの消費電力や電磁波から暗号を解読するサイドチャネル攻撃によって，物理現象から情報が漏れる可能性があります［基本原理は前編（2013年9月号pp.122-130）参照］．

本稿では，市販の一般的なワンチップARMマイコンでシンプルな暗号化ソフトウェアを動作させ，消費電力波形を解析することで鍵が推定できてしまう例を紹介します．

サイドチャネル攻撃の対策についても解説します．