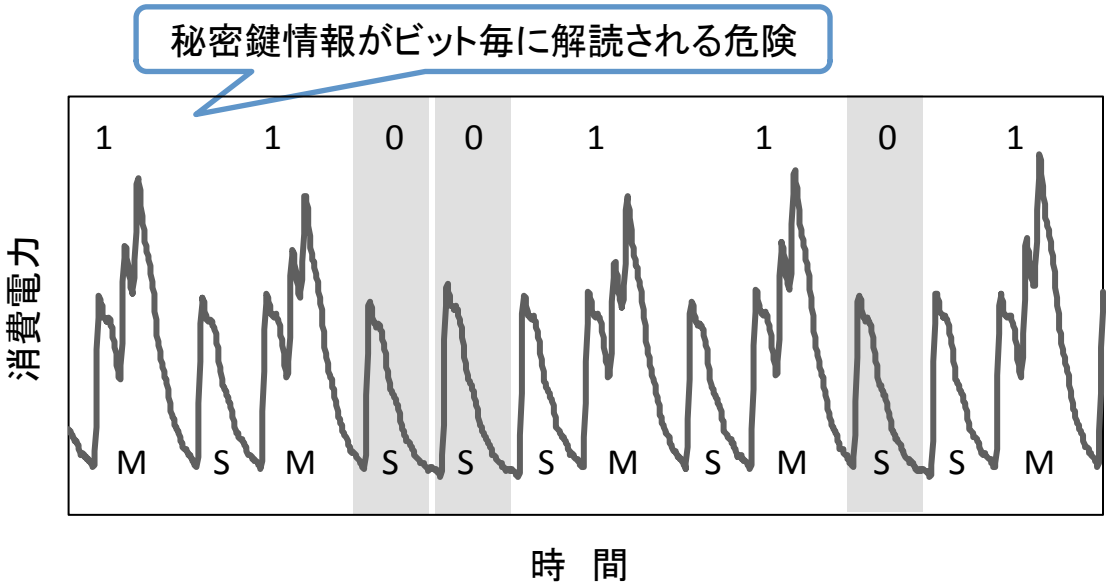
崎山 一男, 太田 和夫, “暗号への脅威「サイドチャネル攻撃」とその対策,”「科学」報告・解説, 岩波書店, Vol.78, No.10, pp. 1080-1083, (2008年10月).訂正箇所

1) 1082ページの図1（解読した秘密鍵）に誤りがありました．正しくは下記の通りです．



2) 1082ページ左カラム中辺り

「実は, M→S のペアが鍵のビット “1” に対応し,S が “0” に対応している.」は，誤りで，正しくは

「実は, S→M のペアが鍵のビット “1” に対応し,S が “0” に対応している.」となります．