暗号処理のソフト vs. ハード

――組み込み用途であれば専用ASICが性能，コストともに優位

佐藤 証，森岡澄夫

ここでは，身近でよく使われるデータ処理である暗号とデータ圧縮を取り上げます．暗号処理としてはRSA(Rivest Shamir Adleman)，DES(Data Encryption Standard)，AES(Advanced Encryption Standard)，またデータ圧縮としてはALDC(Adaptive Lossless Data Compression)について，ハードウェアやソフトウェアとして実装する際に気をつけるべき点，そして両者によって得られる性能について解説します．（筆者）

暗号はデータ通信などを安全に行う目的で用いられ，銀行のオンライン取引，ワイヤレス自動改札，携帯電話の秘話通信，映画や音楽などのディジタル・コンテンツ配信など，応用範囲は多岐にわたっています．ここでは，暗号処理のデファクト・スタンダードであるRSA（Rivest Shamir Adleman），DES（Data Encryption Standard），AES（Advanced Encryption Standard）を取り上げます．

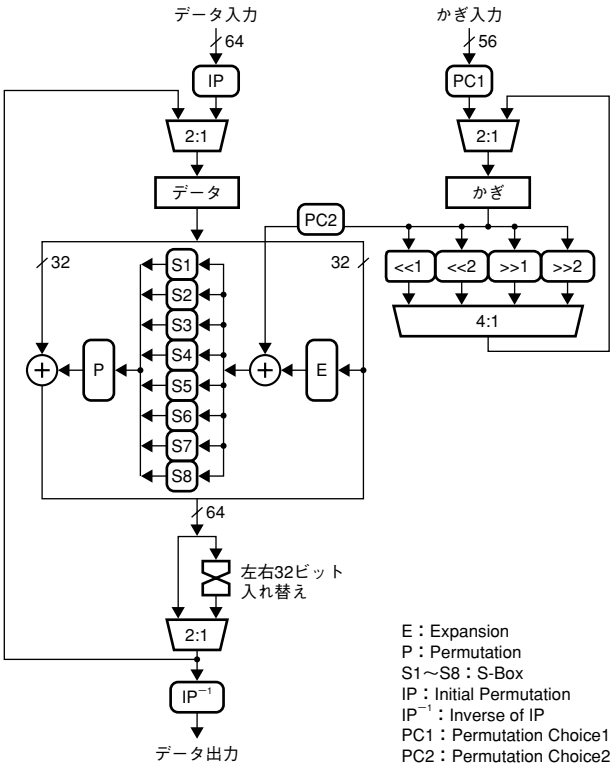
一方，データ圧縮は記憶装置の見かけ上の容量を増加させたり，データ通信に必要な帯域などを減らす目的で用いられます．MPEGやJPEGなどの非可逆圧縮もありますが，ここでは，可逆圧縮でPKZIPにも使用されているスライド辞書法をベースとしたALDC（Adaptive Lossless Data Compression）を取り上げます．

1. 共通かぎ暗号DES，AESのハードvs.ソフト

共通かぎ暗号としては，20年以上にわたって8割以上の暗号製品に使われてきたと言われるDESが有名です．AESはDESに代わる次世代のスタンダードとして，2001年に米国連邦標準局（NIST）が制定したものです．

●基本構造―DESのデータ長は64ビット，AESはその倍

DES，AESのいずれも基本処理はシンプルで，ラウンド関数（round function）と呼ばれるデータ変換処理を一定回数繰り返します．ここでは，この処理1回を1ラウンドと数えることにします．回路の基本構造を図1に示します．図1（a），（b）ともに左半分がラウンド関数部であり，データ



（a）DES, Triple DES

はレジスタに置き，組み合わせ回路に入力して変換を繰り返します．各ラウンドでは，ユーザが設定した「かぎ」から作った情報（ラウンドかぎ）と変換結果のXORをとります．**図1（a），（b）**の各図の右半分が，ラウンドかぎを生成する部分です．

DESとAESでは，1回のラウンドで処理するデータとかぎのビット数が大きく異なります．DESのデータは64ビット，かぎは56ビットです．これに対し，AESのデータは128ビットで，かぎは128，192，256ビットの3種類から選ぶことができます．また，DESとAESではラウンド数やラウンド関数の内容も異なっています．

なお，Triple DESは，基本的にはDESを3回続けて処理する方式で，かぎのビット数を見かけ上DESの3倍にしたものです．

●共通かぎのボトルネックはS-Box

共通かぎ暗号は，単純にラウンド関数を繰り返すだけなので，実装性能は1ラウンドの処理にどれだけの時間をかけるかによって決まることは明らかです．ラウンド関数では，S-Boxと呼ばれる非線形変換のコストがいちばん高く，ここをどう作るかがポイントになります（ラウンド関数の残りは，ビット入れ替えやXORなど，わりと単純な処理である）．

●ハードー1クロック1ラウンドの処理が基本

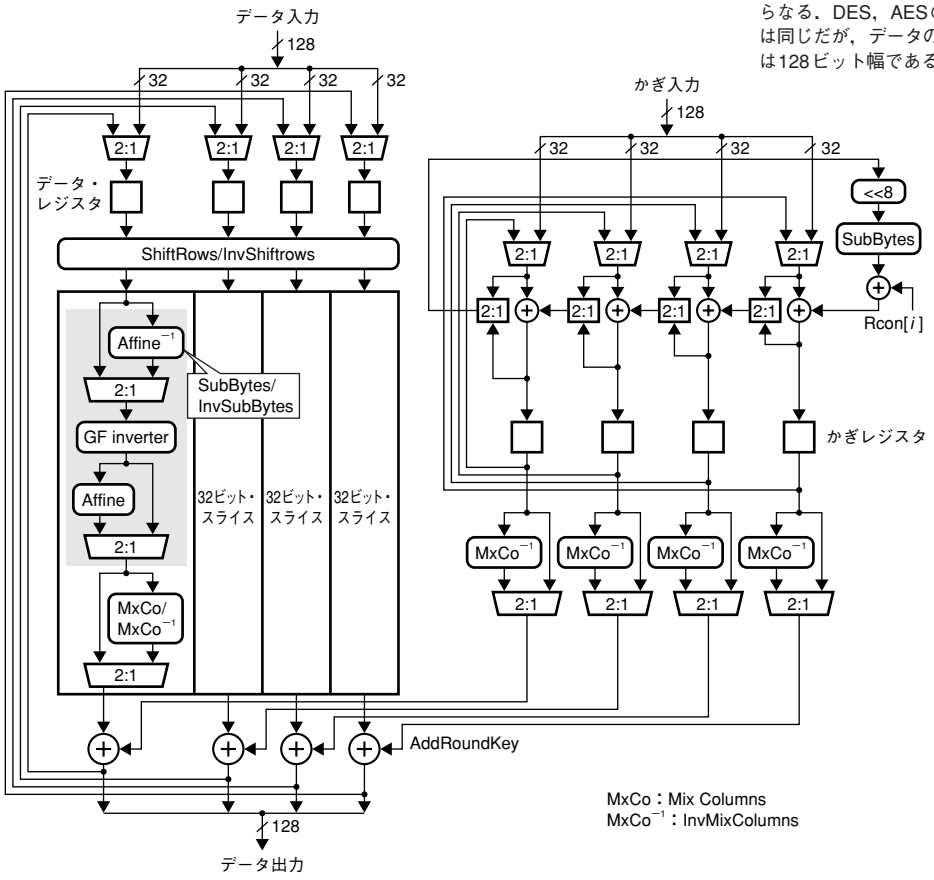
ハードウェア（ASIC）による実装では，1クロックで1ラウンド分の処理を行う方式がもっとも標準的です．この場合，DESでは16クロック，Triple DESでは48クロック，AESでは11クロックかかります．

回路性能を変えるためには，次の2点を調整します．

1）1ラウンドのクロック数（または1クロックで処理するラウンド数）
2）1ラウンド分の処理を行う組み合わせ回路（特にS-Box）

〔図1〕共通かぎ暗号回路の基本構成

共通かぎ暗号回路は，「ラウンド関数」と呼ばれるデータ変換部（左半分）と，データ変換に使う「ラウンドかぎ」を生成する部分（右半分）からなる．DES，AESのいずれもラウンド処理を一定回数繰り返す点は同じだが，データのビット幅が異なる．DESは64ビット幅，AESは128ビット幅である．ラウンドの処理内容ももちろん異なる．



（b）AES