超高速超軽量ストリーム暗号アルゴリズム「KCipher-2」

2006 年 5 月、KDDI、KDDI 研究所、NHK 放送技術研究所は、共通鍵暗号によるデータ暗号化アルゴリズム「KCipher-2（ケイサイファーツー）」を利用して、ワンセグなどのモバイル端末（携帯電話・PDA など）向け放送型サービスに適用可能なコンテンツ保護技術を共同開発した。

「KCipher-2」の最大の特徴は、専用のハードウェア部品を必要とせず、CPU＊を使ってソフトウェアのみで復号化が行えることで、比較的安価で実装でき、さまざまなアプリケーショ（BREW）への適用が可能であること、携帯電話等のモバイル端末の CPU においても、動画像（ワンセグ相当）の複号化を CPU への負荷を抑えてリアルタイム処理を可能としたことである。

携帯電話に実装した実験では、試験機の CPU 使用率は 1%未満に抑えられ、十分実用に耐えるレベルにあることが実証された。加えて、既存の暗号アルゴリズム「AES」（Advanced Encryption Standard）と比較して 6〜8 倍の速さで動作するため、既存方式では不可能であった携帯電話端末でのワンセグ相当の動画像のリアルタイム復号を可能とする高速化を実現した。

リアルタイムにストリーミングを配信する放送型サービスが注目される中、コンテンツ保護技術は不可欠であり、携帯電話などの CPU は PC と比べて処理能力が低いことから、より軽い暗号処理技術が求められていた。また、サービスにおいても PC などとのデータ交換が進むことは必須である。これらの要求に対して、汎用性が高く、携帯電話上で動作可能な「KCipher-2」はコンテンツビジネスの発展に寄与すると期待される。

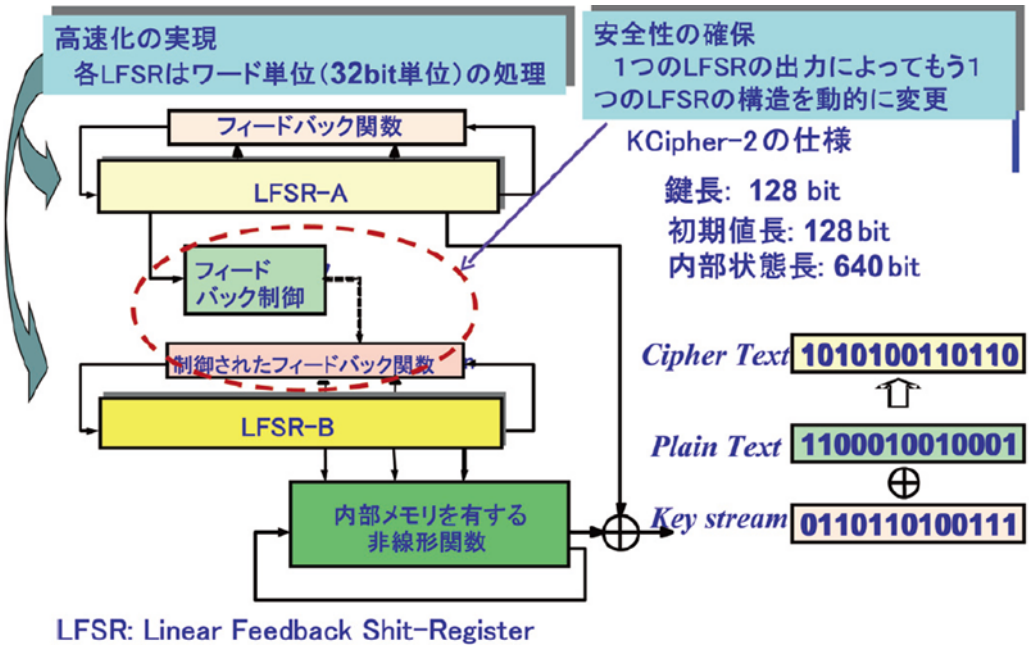

図 「KCipher-2」の処理概要