暗号のシステム応用

秋山, 浩一郎
株式会社東芝研究開発センター

出版情報：COE Lecture Note. 46, pp.301-308, 2013-02-28. Institute of Mathematics for Industry, Kyushu University
バージョン：
権利関係：

暗号のシステム応用

秋山　浩一郎

株式会社東芝　研究開発センター

概 要

暗号は数理的な知見が反映されている技術であるが、それが身近に応用されていることは意外と知られていない。本稿では暗号が応用された事例の中で典型的なものであるDVD/BD（ブルーレイ）向けのコンテンツ保護とクラウドストレージサービスを例にとって解説する。

1　はじめに

暗号は特定の人のみに情報を伝達するアルゴリズムとして、最初は軍事向けに開発された。暗号には大きく分けて共通鍵暗号と公開鍵暗号がある。共通鍵暗号は高速ではあるが、1つの鍵（共有鍵）を共有している相手としか暗号通信できない。公開鍵暗号は低速であるが、公開鍵と呼ばれる不特定多数に公開できる暗号化鍵で暗号化を実現し、秘密鍵を呼ばれる自分だけが知る復号鍵で復号することができる。共通鍵暗号ではデータをビット毎に分解し、スクランブルを行っている。スクランブルのパターンを決めるのが鍵（共通鍵）であり、暗号化で使った鍵を復号で利用しない限り、コンテンツは復号できない。一方、公開鍵暗号は、これに加えて、公開された公開鍵から秘密鍵が求められないという非対称な性質を実現するため [1] で紹介されているような数理が使われている。多くのシステムでは、コンテンツの暗号化には高速な共通鍵暗号を、そこで使われる共通鍵の暗号化には公開鍵暗号を利用する方式（ハイブリッド方式）が取られることが多い。本稿ではこれら暗号のシステム応用に焦点をあて、その代表的な2つの事例を紹介する。

暗号の応用がどのように始まったのかを理解するために、暗号の歴史を簡単に振り返ってみよう。暗号は1960年代までは主に軍事目的で研究され、その内容も軍事機密であり公表されることはあまりなかった。しかし、1970年代後半に公開鍵暗号が開発されるに至って、公開の場での安全性に関する学術的な議論が盛んになり、1980年代後半までには [1] で紹介されているRSA暗号やその安全性など公開鍵暗号の基礎が整備されてきた。その後は1990年代半ばに始まる機器のデジタル化や情報システムのネットワーク化に伴って、暗号は安全を守る技術として広く応用されるようになってきた。応用された身近な例としてSSL (Secure Socket Layer) による通信がある。ここでは、インターネット上で会員登録やショッピングなどをする際、住所やクレジットカード番号などの個人情報を第三者に秘匿する目的で暗号が利用されている。

一方、産業界では1980年代半ばにCDが発売され、それまでにないデジタル音声による、極めてクリアな音が楽しめるようになった。しかし、それまでのアナログ録音とは違ってコピー

すれば全く同じものができてしまうという問題が指摘されていた。実際、CD はこれから述べるようなコピー制御手段を定めずに販売されてしまったため、後にコピー制限を加えるまでは、コピーし放題とも言える状況となった。1996 年に発売された DVD ではその反省を生かし、設計段階からコピー制御機構が検討され、実際にコピー制御機構を導入したものが発売されている。コピー制御は簡単に言うと、コンテンツを暗号化して、コピー制御された機器のみに復号して再生させる仕組みである。ここでは暗号方式に加えて、復号鍵をどのようにコピー制御された機器にのみ渡すか？ という問題がある。このような仕組み全体はコンテンツ保護と呼ばれており、その概要を 2 節で述べる。

一方、2000 年代後半からクラウドと呼ばれる大量の資源を持った計算機環境が提唱されてきた。クラウドではそれら大量の資源を複数の利用者で共有することで、計算機の導入コストを大幅に下げることができる。一方で、他人と共有することからデータを覗き見られる恐れがあるだけでなく、大量のデータが集まることから、サイバー攻撃を受けやすい。そこで、機密性の高いデータを中心に暗号化して保存する方法が取られている。しかし、クラウドの計算機環境を有効に利用するためには、可能な限りクラウド内で処理する必要があり、暗号化したまま処理できる暗号方式が求められている。残念ながら、現状では、全ての処理が暗号化したまま可能となる訳ではなく、実用的な暗号方式を目指した研究が進められている。3 節ではそれら実用的な暗号のうち、再暗号化技術を紹介する。

2　コンテンツ保護

コンテンツ保護の目的は視聴（あるいは閲覧）する権利のある人（通常はコンテンツ購入者）にのみにコンテンツを見る権利を付与することである。映画などの DVD コンテンツを不正コピーされると当該コンテンツを視聴する権利のない人でも見ることができてしまう。このことからコピー制御はコンテンツ保護の中で重要な役割を果たしていることが分かる。しかし、コピーする能力のある録画再生機器を遠隔で監視・制御することはできない。そこでコピー制御では、適切にコピー制御を行う機器にのみコンテンツを視聴させるという手法を採用している。

特定の人（ここでは機器）にのみコンテンツを視聴させるようにするには、コンテンツを共通鍵暗号で暗号化し、そこで使われる鍵を公開鍵暗号で暗号化して送るという手法が一般的であった。しかし、DVD/BD はメディアであるので、メディアに（特定の機器でのみ復号できる形で暗号化して）コンテンツを復号できる共通鍵を書き込んでおく。この共通鍵をメディア鍵という。

本節では、DVD に採用されている CPPM (Content Protection for Prerecorded Media) の仕組みについて解説する。図 1 を見て頂きたい。DVD メディアに書かれているメディア鍵は Lead-in 領域と呼ばれる通常読み込めない領域に機器毎に異なる形で暗号化された鍵束として記録されている。この鍵束を MKB (Media Key Block) と呼んでいる。MKB は多数存在する機器向けのメディア鍵を効率良く暗号化して束にしたもので、単純に機器毎に暗号化したものを束にしたものと比較して、データサイズを圧倒的に小さく抑えることができる。

機器固有の鍵（デバイス鍵）を用いることで MKB からメディアに固有の鍵（メディア鍵）

を復元する（MKB 処理）。メディア鍵はこのメディアに暗号化して記録されているコンテンツを復号するための起点となる鍵である。タイトルを復号するときはタイトルに対応するアルバム ID を DVD から抽出し、アルバム ID とメディア鍵から一方向性関数を利用してアルバム固有鍵を出力する。更に、コンテンツを復号するためにはアルバム固有鍵と 2048 ビット毎に定められた鍵変換データを繰り返し適用することによって、コンテンツ鍵を抽出する必要がある。コンテンツ鍵が出力されれば、それを使ってコンテンツを復号することによって視聴が可能となる。

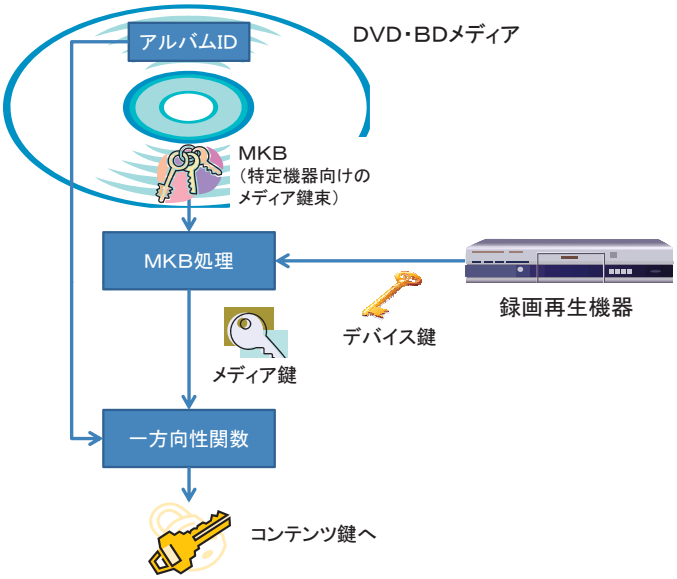

図 1：CPPM の概要

CPPM におけるコンテンツ保護はデバイス鍵が起点となっている。即ち、デバイス鍵が露見してしまうと、そのデバイス鍵を用いることで、メディア鍵が取り出せてしまう。DVD ではデバイス鍵は機種毎に設定されているが、ある機種のデバイス鍵が露見すると、その機種になりすました不正再生ソフトを作ることが可能になる。そのような場合に対抗するため、新たに発売されるメディア（ディスク）からは、その MKB に当該機種向けの鍵を含めないという取り決めがある。即ち、メディア鍵が露見した機種では、新しく発売されるコンテンツを復号できなくなり、新しいコンテンツの不正コピーができないだけでなく、再生もできなくなる。では、新しいコンテンツが再生できなくなった機種はどうするのであろうか？ デバイス鍵が露見した原因を特定した上で、可能ならインターネット経由などでシステム更新を行う。

DVD よりも大容量メディアである BD では、セキュリティを強化したコンテンツ保護方式 AACS (Advanced Access Conent System) が採用されている。BD は DVD よりも容量が大きくなり、高精細で付加価値の高いコンテンツを楽しむことができるようになった。このため、CPPM の実用化により明らかとなった問題点を改善するセキュリティ機能を盛り込んだ方式

となっている。ここでは、それらの機能のうちの 2 つを紹介する。

- 再生機器を同定する機構 (Sequence Key Block)
  CPPM では不正機器を特定することが困難であった。この反省から再生されたコンテンツから再生機器を特定できる機構を導入した。再生機器にシーケンス鍵セットを持たせ、これらシーケンス鍵によって、復号されるコンテンツが異なるようにしておく。異なるコンテンツと言っても内容が異なっては困るので、電子透かし[1]などを使って人間の目に分からない程度に差異を設けておくのである。
- 不正コンテンツの無効化（コンテンツ証明書）
  CPPM ではコピー防止はできたが、海賊版などの不正コンテンツも再生できてしまうという問題があった。そこで AACS では正当なコンテンツに対しては証明書（コンテンツ証明書）を付与することになった。コンテンツ証明書は機器に備えられている公開鍵で認証することで正当なコンテンツであることが分かり、正当なコンテンツのみを再生できるようになった。

3　クラウド向け暗号

クラウドは大量の計算機と大きな記憶容量を備えた計算環境である。利用者は利用するソフトウェアやデータも含めて処理に関係するほとんど全ての部分をクラウド側に持たせて処理することができる。このため、利用者はネットワークに接続可能なクライアント端末（PC 等）以外の設備投資をすることがなく、導入コストを下げられるため、近年個人も含めて利用が進んでいる。

一方で、クラウドには多くのデータが集まるためサイバー攻撃の対象となりやすい。そのため、外部からの侵入を防止するための数々のセキュリティ対策が取られている。しかし、サイバー攻撃も日に日に進歩しているため、常に新しい攻撃が出現する。そこで、（個人情報等の）漏れてはいけないデータをクラウドで処理するためには、暗号化して保管することが必須である。暗号化して保管したものは（通常は）復号しないと処理することができないが、クラウド上で復号するとサイバー攻撃を受けやすい。その一方で、クライアントで復号する場合、クラウドからデータを転送する必要があり、大容量のデータであればあるほど、現実的ではない。

そこで、暗号化したまま処理可能な方式があれば理想的である。実際に、暗号化したまま共有する方式、暗号化したまま演算する方式、暗号化したまま検索する方式が知られている。

暗号化したまま共有する方式には、暗号文を（復号する個人向けに）変換する技術と、（復号できるグループ向けに）暗号化する技術が知られている。前者は再暗号化技術と呼ばれ、元の暗号文の変換を基本とするためアクセス権を変更しやすいが、変換のための再暗号化鍵が必要であり、それを管理する管理サーバが必要である。後者は予め定められたグループの人のみが復号できる形で暗号化する技術で、管理サーバの必要はないが、グループの構成メンバに変更があった場合は対応が難しい。

暗号化したまま演算する方式は（完全）準同型暗号と呼ばれ、暗号化したまま足し算と引き算ができる方式を準同型暗号、掛け算も可能な方式を完全準同型暗号という。準同型暗号は、

[1]画像の一部に人目では分からないような情報を埋め込む技術

その名の通り、暗号化関数が準同型性を持つ暗号方式である。即ち、暗号化関数を E とするとき、

$$E(x) + E(y) = E(x + y)$$

という性質を満たすのが準同型暗号、

$$E(x)E(y) = E(xy)$$

も満たすのが完全準同型暗号である。式を見れば明らかなように暗号化された数値同士を足し算、掛け算した結果が、(暗号化していない) 数値同士を足し算、掛け算したものを暗号化した暗号文となっている。これを複数回組み合わせることで、大量の (暗号化された) データの足し算や掛け算をすることができる。準同型暗号を実現する暗号方式には格子暗号などが知られている。

暗号化したまま検索する方式は検索可能暗号と呼ばれており、テキスト文書の中のキーワードを暗号化したまま検索する方式である。応用先によっては検索するキーワードも秘匿したいという要求もあり、検索するキーワードを秘匿する方式も多い。

本節では特に再暗号化技術を取り上げて原理を詳しく説明する。再暗号化技術は暗号文を (復号する個人向けに) 変換する技術である。図 2 を見て欲しい。取引先の担当者がプロジェクトグループのメンバに文書を送る際、管理者 X からそのプロジェクトグループに割り当てられた公開鍵で暗号化してクラウドにアップロードする。再暗号化サーバは再暗号化鍵を使ってグループのメンバが復号できるような形に変換する。例えばメンバ A 向けに再暗号化鍵 $K_{X \to A}$ を使ってメンバ A の秘密鍵で復号できるような形に変換する。このようにすることで、メンバは個別の鍵 (秘密鍵) を持ちながら同じ暗号化データを共有することができる。

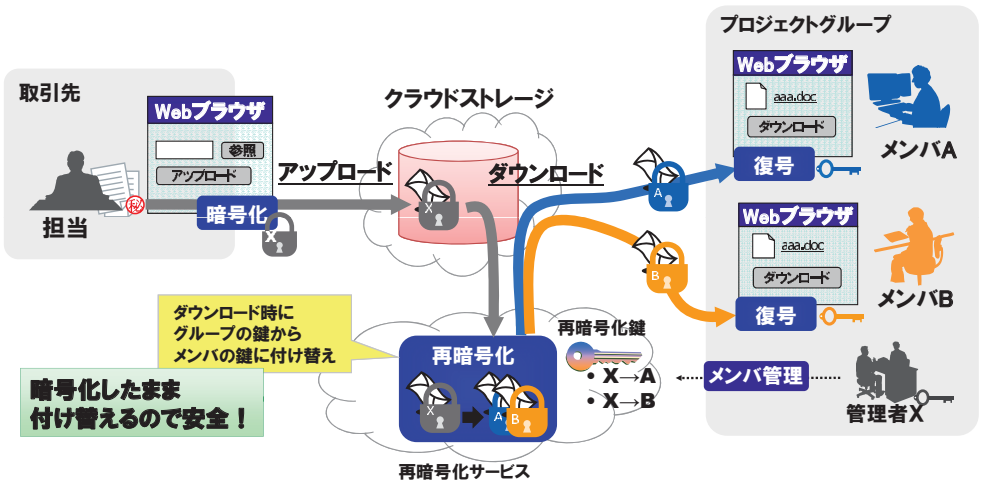

図 2：再暗号化

このような特性を持った暗号はペアリングを利用して構成する。ペアリングとは楕円曲線 E/F_p の上の 2 点 P, Q のペアで定義される量 $e(P, Q)$ であり、楕円曲線の定義体 F_p の拡大体 F_{p^k} 上に値を取る。

楕円曲線上の点には加算（点加算）が定義できるので、2 点 P, Q に対して $P+Q$ が計算できる。実際にどのように計算するのかは [1] に記述があるので、そちらを参照願いたい。同様に同じ点の加算もできるので P の 2 倍点 $2P = P + P$ も定義できる。更に $3P = 2P + P$ が計算できることを考えると a を正整数としたとき、点 P の a 倍点 aP も計算できる。また、$P = (x, y)$ に対して $-P = (x, -y)$ と定義できるため、更に一般化して、a を非零整数としたとき、点 P の a 倍点 aP も計算できることになる。このような演算を点 P のスカラー倍算と呼ぶ。このようなスカラー倍をした点 aP, bQ に対して、ペアリングは下記のような性質を満たす。

$$e(aP, bQ) = e(P, Q)^{ab}$$

この性質は双線形性と呼ばれる。

これを使って、まずは再暗号化の暗復号アルゴリズムを紹介する。

[システムパラメータ]

素数位数 l の楕円曲線 E/F_p とその生成元を P とする。生成については [1] を参照。この楕円曲線 E/F_p 上で定義されるペアリング $e(P, P)$ が含まれる有限体を $K\ (= F_{p^k})$ とおく。

[公開鍵および秘密鍵]

秘密鍵 $s \in \{1, 2, \ldots, l-1\}$ に対して、$Q_s = sP$ を公開鍵とする。

[暗号化]

平文 m を有限体 K の元とする。乱数 $r \in \{1, 2, \ldots, l-1\}$ を発生して、システムパラメータ P と公開鍵 Q_s を使って、

$$C_1 = rQ_s \in E/F_p, \quad c_2 = m \cdot e(P, P)^r$$

を計算し、(C_1, c_2) を暗号文とする。

[復号]

暗号文 (C_1, c_2) に対して、秘密鍵 s を利用して、復号

$$c_2/e(s^{-1}C_1, P) = m \cdot e(P, P)^r / e(s^{-1}rsP, P) = m \cdot e(P, P)^r / e(P, P)^r = m$$

を行う。

次に、再暗号化の主要部分、暗号文を（復号する個人向けに）変換する再暗号化処理と、その復号について詳しく説明する。

[システムパラメータ]

前記と同じ。

[（個人（メンバ A）向けの）公開鍵および秘密鍵]

秘密鍵 $a \in \{1, 2, \ldots, l-1\}$ に対して、$Q_a = aP$ を公開鍵とする。

[再暗号化鍵]

$(a/s)P$.

［（メンバ A 向けの）再暗号化］
暗号文 $(C_1, c_2) = (rQ_s, m \cdot e(P,P)^r)$ に対して、メンバ A 向けの再暗号化鍵 $(a/s)P$ を利用して $e(C_1, (a/s)P)$ を計算する。これは

$$e(rQ_s, (a/s)P) = e(rsP, (a/s)P) = e(P,P)^{ar}$$

となり、これを C_{1A} とする。c_{2A} は c_2 をそのまま継承して、暗号文 (C_1, c_2) はメンバ A 向けの暗号文 $(C_{1A}, c_{2A}) = (e(P,P)^{ar}, m \cdot e(P,P)^r)$ に変換される。

［復号］
秘密鍵 a を使って、

$$\frac{c_{2A}}{C_{1A}^{a^{-1}}} = m\frac{e(P,P)^r}{e(P,P)^r} = m$$

により復号される。

再暗号化方式はメンバに個別の鍵を持たせ、データへのアクセス制御を再暗号化サーバで管理できるため、組織変更などによるメンバの脱退・加入に対応しやすいという特質があり、クラウドストレージサービスとして実用化されている。今後の発展が楽しみな技術である。

4　おわりに

本稿では、数理的に構成された暗号が実際のシステムに応用されている典型的な事例を紹介した。暗号技術は情報セキュリティの主要技術であるため、今後とも活用が進むと考えられる。これからは新興国を中心に電気・ガス・水道・交通などの社会インフラがインターネットに繋がっていくため、これらに向けた活用が進むものと考えられる。これらのシステムは、機器や施設を制御するため、非権限者によりシステムが勝手に操作されることを避けなければならない。即ち、権限者と非権限者を分けるための仕組みが重要となる。このような仕組みは認証と呼ばれ、やはり暗号技術により構成される。

また、暗号実装のことにも少し触れておかなくてはいけない。暗号はアルゴリズムレベルで安全であっても実装により鍵が漏れることがある。たとえば、暗号をソフトウェアで実装した場合、鍵がソフトウェア内部に存在すれば、デバッグツールなどを使って解析することにより露見してしまう。ハードウェアで実装した場合でも、ハードウェア内部には鍵があり、その鍵を使って暗復号処理が進むので、その消費電力波形から鍵が漏れることがある。なぜなら、鍵により処理パターンが決まり、その処理パターンにより消費電力が変化するからである。最近のシステムでは、このような攻撃にも対抗できる方式が用いられている。

このように、暗号への攻撃（解読）の試みも進められており、常に最新の技術を参照しながらシステム開発やメンテナンスをしていく必要がある。

参考文献

[1] 高木剛，公開鍵暗号入門，本書所収.