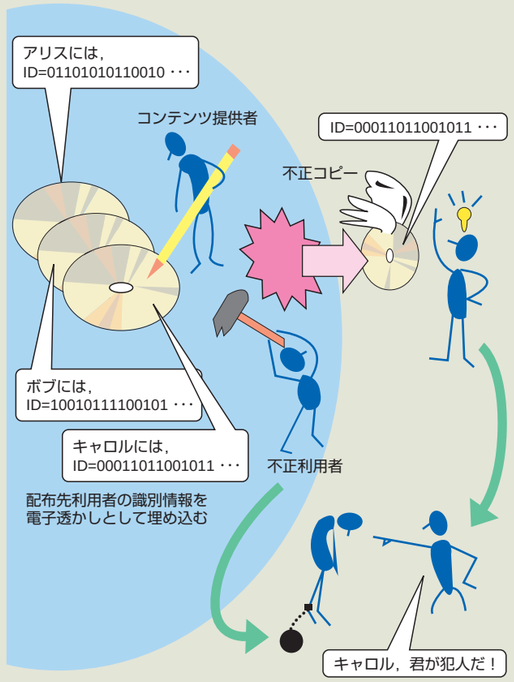
動画コンテンツの不正コピー流出を防止するフィンガープリンティング

結託により作られた不正コピーに対する出所追跡能力を大きく向上

デジタルコンテンツの不正コピーを抑止する目的で，コンテンツに利用者識別情報を埋め込むフィンガープリンティングが提案されています。しかし，不正な利用者が複数人集まり，結託してコンテンツに埋め込まれた識別情報を解析し，それを消去・改ざんするおそれがあります。

東芝は，そのような“結託攻撃”に対して強い識別情報符号の構成法を提案しました。従来の構成法に比べ，符号長を著しく短縮しているのが特長です。



ID：識別情報

図1．フィンガープリンティング ― 識別情報をコンテンツに埋め込んでおき，不正コピーが流通した際には，その出所を特定するスキームがフィンガープリンティングで，結託攻撃に対する耐性が必要です。

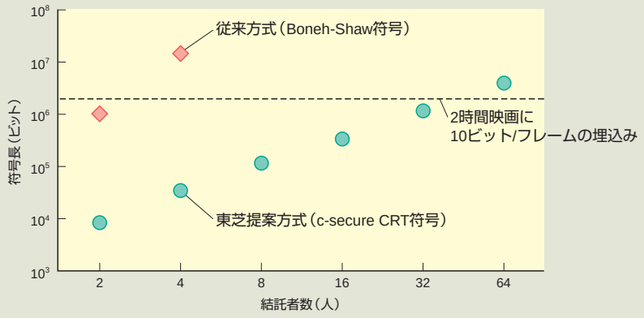


図2．c-secure CRT符号による符号長の短縮 ― 当社提案方式は従来方式に比べ符号長が1/100以下に短縮されている。

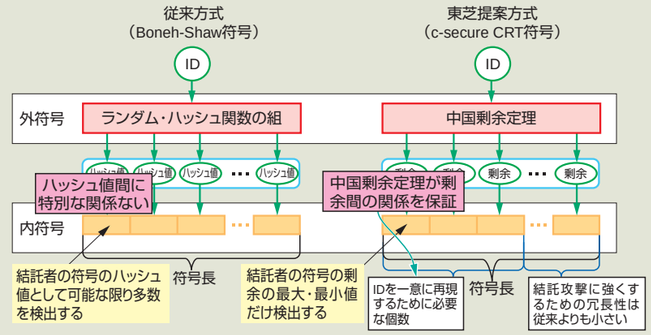


図3．c-secure CRT符号の構造 ― c-seucre CRT符号は，中国剰余定理によって剰余間の関係が保証されるため，冗長部を小さくでき，符号長を短かくすることができます。

コンテンツ配信の著作権保護

音楽や映画などのネットワーク配信では著作権保護が重要です。既に，様々な仕組みを施した安全な配信システムが提案され，実際の配信サービスに用いられ始めています。

しかし，安全なシステムを構築する努力が払われる一方で，必ず，それを破ろうとする者が現れます。万一，その仕組みが破られたとき，不正コンテンツが流通するおそれがあります。

そのような不正に対抗するため“フィンガープリンティング”という手段が提案されています（**図1**）。

これは，コンテンツ提供者が利用者を特定する識別情報を“電子透かし”としてコンテンツに埋め込んでおき，不正コンテンツが現れたときは，埋め込まれている電子透かしを検出し，その出所を特定する方式です。

識別情報が埋め込まれたコンテンツがそのまま海賊版として流通する場合には不正者を特定できますが，次のような場合には問題です。

それは，複数の利用者が共謀して各自に配布されたコンテンツを持ち寄り，比較して電子透かしの埋め込み方法を解析し，それを削除又は改ざんする“結託攻撃”が行われた場合です。

価値があるコンテンツの場合，結託攻撃をしてまで海賊版を配布する不正者が現れるおそれがあります。

結託攻撃に強い符号

1995年にプリンストン大学の研究者が，結託攻撃に強い識別情報符号を提案しました。識別情報を2元符号に符号化し，その符号を電子透かしとしてコンテンツに埋め込みます。この符号（c-secure符号と呼ばれる）は，“結託者の人数があるしきい値（c人）以下であれば，結託攻撃によって作られた不正コンテンツから検出した電子透かしから，結託者のうち少なくともひとりの識別情報を検知できる”働きをします。

しかし，この符号構成法は符号長が大きく，実用的ではありませんでした。

東芝提案方式

東芝は，新しく“c-secure CRT符号”を提案しました。従来の構成法（Boneh-Shaw符号）に比べ，符号長を約1/100以下に短縮することに成功しています（**図2**）。例えば，映画（2時間の動画コンテンツ）ならば，1フレーム当たり10ビットの埋込みで，ユーザー数が10億人のとき結託者数40人までであれば，少なくともひとりを追跡可能です。これは従来，数百時間のコンテンツでないと達成できなかった追跡能力です。

当社の提案方式では，中国剰余定理（CRT：Chinese Reminder Theorem）を利用して符号が構成されます（**図3**）。中国剰余定理は，古代中国の孫子算経という書物に既に記載がある古くから知られている定理で，ある数は，いくつかの互いに素な整数でその数を割った余り（剰余）の組によって一意に表されるというものです。

符号化処理の中で，まず，識別情報は剰余の組で表現され，次に，各剰余は，結託者の剰余の中の最大値と最小値を検出できる符号により符号化されます。そして，各剰余から得られた符号語をつなぎ合わせ，識別情報の符号語とします。

結託者の追跡時には，まず，符号語をコンテンツから読み取り，互いに素な整数の各々に対して，結託者の剰余の中の最大値と最小値を復号します。

中国剰余定理により，一定の個数以上の剰余がある結託者のものであるとわかれば，結託者の識別情報を一意に再現できるのですが，剰余の最大値及び最小値のどの組合せが同一の結託者に由来するものかがわからないと，中国剰余定理が適用できません。ところが，興味深いことに，互いに素な整数の個数がある条件を満たすだけ多くなると，あるしきい値以上の個数の最大剰余，最小剰余と同じ剰余を与える識別情報は，非常に高い確率で結託者の識別情報であることが証明できるのです。こうして，c-secure CRT 符号は，中国剰余定理をうまく応用することにより，世界最短の符号長を与えています。この追跡方法の正しさの証明を情報ハイディング技術に関する国際会議IH2001で，また，各種の改良を施すことで，符号長を更に約1けた短縮できることをIH2004で発表しました。

実用化への課題

符号長を著しく短縮できたとはいえ，実用化には，符号長の更なる短縮が必要です。また，この符号を生かすシステムの検討も必要です。今後も継続して，これらの課題へ取り組んでいきます。

村谷　博文

研究開発センター
コンピュータ・ネットワークラボラトリー
主任研究員