放送型配信における鍵漏洩抑止スキームの拡張
～一対多の暗号方式～

1　背景

急速に IT 化が進みつつある現代では個人や法人を問わず様々な面において暗号に関する技術は必要不可欠である。今後電子取引や電子マネーなどが普及するとますますその重要度は増してくる。しかし、その暗号基盤技術を提供する会社となると、海外には RSA Data Security や F-secure などがあるが、日本には世界標準の技術を請け負う有力な会社がなく、技術はあっても学者の中の理論で閉じてしまっているものが多い。これは日本の大企業が技術を自社内に抱え込んでしまう体制、また日本発の技術を信頼、信用して使用しないという体制に一因があると思われる。日本発の技術であるにもかかわらず海外で先に評価され、逆輸入されたケースはよく見受けられる。そこで日本の中でアイディアとしてだけ存在していた暗号技術を形にし、世界に送り出すことを目的とした新規企業を設立したい。それにより後発であった暗号技術に関しても世界標準を目指し「技術大国日本」を築く一助としたい。

昨年末より地上波ディジタルテレビやディジタルラジオ放送が始り、コンテンツ保護の重要性が高まっている。ここではそういった際に必要な不正受信及び不正受信装置の作成を困難にさせる通信方式の実装を行なう。

2　目的

昨年度に未踏ソフトウェア創造事業で採択された案件を改良し成果を公開可能な形で提供する。

3 開発の内容

3.1 概要

コンテンツ配信者が、暗号鍵は一つで各ユーザに渡す復号鍵を任意個生成でき、更にその復号鍵に各ユーザの識別情報を埋め込むことが出来るシステムを作成する。またある範囲内で特定のユーザの鍵を無効化する鍵排除機能を追加する。それらを利用できる簡単な Windows GUI アプリケーションを作成する。

コアとなるペアリング演算部分は、昨年度開発した多倍長演算ルーチンを下位ルーチンとし、それを利用する上位ルーチンを C++ テンプレートライブラリの形で提供できるように再設計した。下位の多倍長演算ルーチンと上位のテンプレートライブラリは独立性が高いため再利用しやすい。

3.2 全体構成と動作環境

有限体上の楕円曲線上の加算及びペアリング演算の実装を行った。更にそれを利用してセッション鍵生成、暗号化、復号、鍵排除機能を持つ C++ のライブラリにまとめた。実際にコンテンツを暗号化する部分には AES に採用された Rijindael 暗号を採用した。以下に挙げる組み合わせで動作する。

ハードウェア	OS	コンパイラ	アセンブラ
AT 互換機	Windows	Visual Studio.Net2003	nasm
AT 互換機	Windows	Intel C++ 7.0	nasm
AT 互換機	Linux	gcc 3.3	nasm
Macintosh	MacOS X	gcc 3.1	—

Windows 版は DLL の形で提供され、その DLL の作成には Visual Studio.Net2003 が必要だが、DLL 自体は Visual Studio 6 からも利用可能である。また実験的に復号ルーチンを Windows の DirectShow のフィルタの形で作成した。これにより例えば暗号化された mp3 ファイルを Multi Media Player からシームレスに扱うことが出来る。

3.3 速度評価

上位側のテンプレートライブラリは同一のまま、下位の多倍長演算ルーチンに我々が作成したものと汎用多倍長演算ルーチンである GMP ライブラリを利用したものを比較したところ、ペアリング演算において約 7 倍の速度を達成できた。これにより専用ルーチンの必要性が明確になった。

3.4 パラメータ生成支援ツールの実装

上記専用ルーチンの作成に必要な各種パラメータ（高速な演算に向いた素数）を生成する補助ツールを作成した。

4 従来の技術（または機能）との相違

Pentium4 SSE2 を利用した高速なペアリング演算ルーチンの実装。ペアリング演算は署名にも使われるなど最近注目度が高い[*1]ため高速な実装が望まれている。また、あらかじめ排除人数の最大値を決めておくという制限はあるが、鍵を配布した後に特定のユーザの鍵を無効化する鍵排除機能を実装した。これは普通の暗号には見られない機能である。

5 普及（または活用）の見通し

背景で述べた放送型有料コンテンツ配信システムにおいて本システムをどのように広めるかがポイントとなる。

6 開発者名

渡辺秀行（アイビス：watanabe@ibis.ne.jp）
光成滋生（ピクセラ：herumi@nifty.com）
石田計（サムス）
高島研也（ユーテンネットワークス）

`http://homepage1.nifty.com/herumi/mtt/index.html` で公開予定。

[*1] F. Zhang, R. Safavi-Naini, W. Susilo, *An Efficient Signature Scheme from Bilinear Pairings and Its Applications*, Public Key Cryptography 2004, pp. 277–290