楕円曲線暗号実装方式CRESERC

1．CRESERC誕生

2003年７月，日本電信電話㈱及び㈱日立製作所と共同で“CRESERC（クレサーク）”を開発した。CRESERCとは，楕円（だえん）曲線デジタル署名方式ECDSA（Elliptic Curve Digital Signature Algorithm）の安全かつ高速な実装方式である。安全性と高速性の両方を兼ね備えるという，これまで実現困難であった実装方式の研究開発に成功した。本稿では，CRESERCの概要を説明する。

2．楕円曲線デジタル署名方式ECDSA

CRESERCは，前述のように楕円曲線デジタル署名方式ECDSAの実装方式である。デジタル署名は，デジタルデータの世界で印鑑や印鑑証明を実現するための技術であり，「e−Japan重点計画」で挙げられている電子政府の実現のために欠かせない暗号要素技術の一つである。また，2001年には日本でもデジタル署名及び認証業務に関する法律が施行され，デジタル署名が通常の印鑑と同等に通用する法的基盤が整備された。電子署名法にかかわる指針には，使用するデジタル署名方式が具体的に幾つか指定されている。ECDSAは，指針に記載されたデジタル署名方式の一つである。また，ECDSAは，日本の電子政府における調達のための推奨すべき暗号（電子政府推奨暗号）の一つに挙げられた方式でもある。さらに，IEEE，ANSI，NESSIEなどあらゆる国際標準にも採択されている。

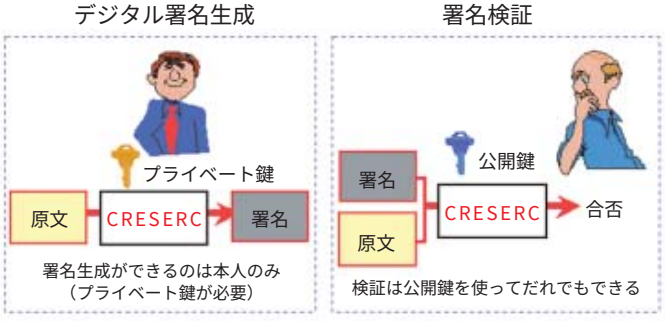
現在実用化が進んでいるデジタル署名方式には，RSA方式とECDSAの２つがある。ECDSAは，RSA方式よりも暗号鍵（かぎ）の長さを短くできる利点がある。現在RSA方式の鍵長は1,024ビット以上が推奨されているが，ECDSAでは，160ビットの鍵でRSA方式の1,024ビット鍵の場合と同等の安全性が達成できる。デジタル署名処理は，鍵のビット長の３乗に比例して処理時間が長くなるため，鍵長が短くできる利点は大きい。将来，暗号解読に用いる計算機の性能が向上し必要とされる鍵長がより大きくなった場合，ECDSAの利点がより一層増してくる。RSA方式で2,048ビット鍵が必要になった場合，それと同等の安全性を達成するECDSAの鍵はわずか256ビットですむと言われている。

3．安全かつ高速な実装

ECDSAは，“楕円曲線離散対数問題”と呼ばれる数学の問題を解くことが難しいということに安全性の根拠を置いている。ECDSAに限らず，暗号アルゴリズムば“数学的安全性”をよりどころにして設計されることが不可欠要件である。一方，1996年ごろから数学的安全性とは別な観点での安全性がクローズアップされるようになった。それがCRESERCが目指した“実装上の安全性”である。暗号は紀元前の昔から使われ続けているが，現代ではコンピュータソフトウェアやハードウェアとして具現化され，様々なMPUやLSI上で動作している。暗号が動作しているデバイスから観測できる電力消費量や暗号処理時間など，データそのものとは違う，いわゆるサイドチャネル情報を利用した暗号解読手法“サイドチャネル攻撃”がある。デジタル署名などの暗号演算は，暗号鍵など第三者に知られてはならない秘密情報を用いて行われる。暗号処理中のデバイスから観測されるサイドチャネル情報が秘密情報と何らかの相関性を持つ場合，暗号解読につながる可能性がある。サイドチャネル攻撃は，数学的暗号解析（攻撃）よりもしばしば強力な暗号解読法となり，現実的な脅威となっている。したがって，その対策が急務であった。サイドチャネル攻撃を防ぐには，秘密情報がサイドチャネルから漏洩（ろうえい）しないような“安全な実装法”を開発する必要がある。これまでにも様々な実装法の研究があったが，安全に実装する際に常に問題になるのは，高速性との兼ね合いである。安全性を考慮した場合，一般的には高速性が犠牲になる。CRESERCは，安全性と高速性の両方を達成したECDSAの実装方式である。

4．CRESERCの今後

CRESERCは，組み込みマイコンからハイエンドCPU，LSIなど様々なプラットフォームに展開可能であり，今後様々な情報セキュリティ製品に展開していく予定である。



CRESERCを用いたデジタル署名

次世代光伝送技術

波長多重(WDM)伝送技術を用いた光通信ネットワークの大規模化が進むにつれて，装置コスト・運用コストを低減するための技術の重要性がますます高まっている。40Gbps波長多重伝送技術は現行の10Gbps波長多重方式と比較して波長数を４分の１に低減できるため，装置規模を小さくするだけでなく，保守・運用を容易にする。また，誤り訂正技術は，機器コストを上昇させることなくシステムの長距離化・大容量化を実現する。これら２つの技術開発について紹介する。

1. 40Gbps波長多重伝送技術

陸上幹線系伝送システム，海底ケーブル光伝送システムへの適用を目指して40Gbps波長多重伝送技術を開発し，世界で初めて再生中継を行うことなく太平洋横断距離の伝送(9,400km)に成功した。それぞれ40Gbpsの情報量を持つ40波長を１本のファイバ上に波長多重伝送することで，合計の伝送容量1.6Tbpsを達成している。現行の10Gbpsの信号と比較して，40Gbpsの信号は，光ファイバ中の非線形効果により品質が劣化しやすく，従来は6,500kmが最長記録であった。新たに開発し適用した技術は次のとおりである。

(1) 超高速光・電子デバイス：40Gbpsで動作する光信号変調デバイス，受信デバイス，信号処理デバイスを開発

(2) 変復調方式：感度を改善するRZ−DPSK(Return to Zero Differential Phase Shift Keying)方式を実装

(3) 中継増幅方式：雑音の蓄積が小さい光ラマン増幅中継技術を採用。２波長励起により利得平坦(へいたん)化を実現

(4) 伝送路技術：非線形効果を抑圧する対称型分散マネジメント光ファイバ伝送路を設計・検証

2. 誤り訂正技術

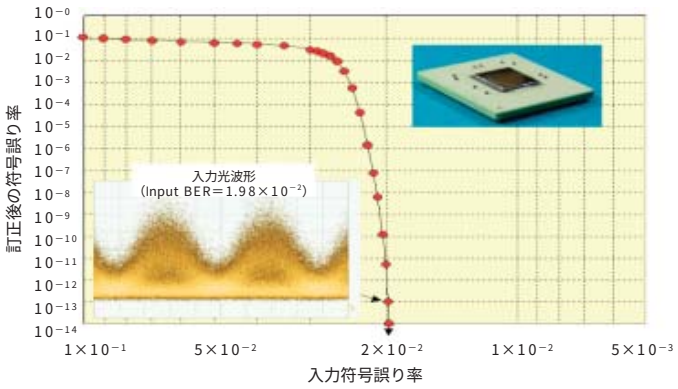
光ネットワークが長距離化・大容量化するにつれて，伝送する情報１ビット当たりの光パワーが減少するため，受信局に正しく情報が伝わらない“ビット誤り”が増加する。システムの高信頼化と低コスト化を実現するためにはビット誤りを訂正する能力の改善が求められている。当社は，世界最高性能の“誤り訂正技術”を開発し，10Gbpsの通信速度での動作実証に成功した。業界標準技術の140倍のビット誤りを訂正できるため，光通信装置のコストを上昇させることなく，システムの長距離化・大容量化が可能となる。主な特長は次のとおりである。

(1) 世界最高の誤り訂正能力：情報ビット全体に対する訂正可能ビット数の比率は最大２％(業界標準は0.014％)。既存システムの伝送容量を３倍，又は伝送距離を1.4倍に拡大することが可能

(2) “ターボ符号”と“軟判定回路”技術：独自の符号処理方式と高速半導体回路設計技術により，従来は高速化が困難とされていた技術を業界で初めて超高速光通信システムで実証

40Gbps波長多重伝送技術，誤り訂正技術は単独で用いることも，組み合わせてもシステムに適用することも可能である。

40Gbps送受信装置と光中継伝送試験系



誤り訂正回路の特性

ナレッジプロバイダー（文書知識活用技術）

企業内に蓄積された文書やインターネットを通して得られる情報からビジネスに有効な知識を的確に抽出・提供するナレッジマネジメントシステムの普及が期待されている。ナレッジ活用ツールとして従来から様々な文書管理ソフトウェアや検索エンジンが提供されているが，①企業内文書には図面や手書き文書など多種多様な文書があり，すべての文書を一括して検索できない，②単なる検索機能だけでは大量の文書中に埋もれたニーズやノウハウなどの知識を抽出する手がかりが得られない，などの課題があった。

これらの課題を解決するため，社内外のあらゆる文書を自動的に登録するとともに自由に検索ができ，概念を自動抽出することでアンケートなどの大量文書から意見・要望を抽出・分析できるナレッジプロバイダー（文書知識活用技術）を開発した。ナレッジプロバイダーは，文書の“検索”“分析”“情報可視化”の３つの要素技術からなる。以下に各要素技術の特長を示す。

1．ナレッジプロバイダーの特長

⑴　検索（文書自動登録・全文検索技術）

イメージ文書・Word・PDF・CADなどの様々な文書からテキストデータを自動抽出するとともに画像データを文字認識によりコード化し，検索索引を自動的に生成する技術を開発した。これにより，イメージ文書はスキャナで入力するだけ，電子文書は所定のフォルダにコピーするだけで全文検索することができる。また，検索結果はページ単位にレイアウト情報も含めて忠実に表示し，同一画面上にキーワードと照合した位置を表示することができる。

⑵　分析（概念抽出・テキストマイニング技術）

文書中の近傍に同時に出現する単語や複合語の傾向を特異値分解手法により解析し，言葉の間の関連性（概念）を自動的に学習する方式を開発した。この方式により，類義語辞書を用いることなく表現が異なる類似文書を検索することや，多様な表現を含む文書の中から言葉の法則性を見付けだすことが可能となる。その結果，アンケート調査の自由意見のように数値で表現できないテキスト情報からニーズを抽出し，マーケティングなどに活用できる。

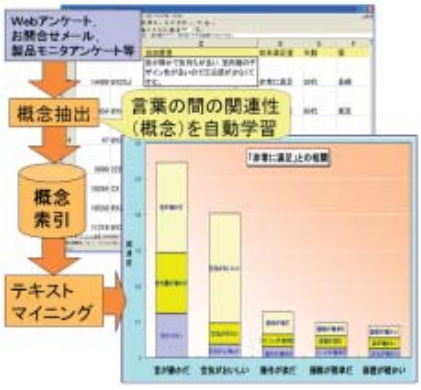
⑶　情報可視化（文書属性抽出・マッピング表示技術）

非定型の文書から属性（日付，部品名など）を自動的に抽出する技術を開発した。この属性情報を基に文書を様々な視点で絵や写真上にマッピングすることで，文書の傾向を直感的に把握でき，大量な文書から所望の文書を簡単に検索することができる。

2．関連製品

ナレッジプロバイダーの文書検索関連技術は，設備情報管理システム，電子納品システム，設備機器のリモート保守ポータルシステムなどの社会インフラシステムに広く応用されている。テキストマイニング技術は，㈱アイプラネットのソリューションサービス“MINING Plus”に適用され，アンケート分析・マーケティング支援サービスに活用されている。また，三菱電機インフォメーションシステムズ㈱では，ナレッジプロバイダーエンジンを搭載した統合ドキュメント管理システム“Manedge Leader”を製品展開している。

イメージ文書（手書き）に対する検索結果表示の例（javaで検索）



エアコンのアンケートに対する分析結果の例

リアルタイム風速分布計測ドップラーライダ

1. 概　　要

レーザ光により風速を測定するドップラーライダは，これまで測定手段がなかった大気中の細かい気流の構造や乱流などの測定を可能とするため，空気の循環や大気汚染の変化を観測する都市環境計測，空港の乱気流を計測して航空機の安全を図る航空管制，風力発電候補地の風況調査等，様々な用途が期待される。また，晴天での計測性に優れており，雨天での計測が主であるドップラーレーダと相補完的にも使用可能である。当社では，これまで，世界に先駆けて，目に対して最も安全なレーザ光の波長帯である1.5μm帯を用いたドップラーライダの開発に成功している。しかし，レーザからの送信パルスの繰り返し周波数が低く，リアルタイム計測性に課題を残していた。今回，送信パルス発生方式の見直しにより送信パルスの高繰り返し化を図るとともに，信号処理装置の高速化を図ることで，長距離の三次元風速分布観測を世界最速の更新レートで行うドップラーライダを実現した。

2. 開 発 概 要

従来，パルス固体レーザで発生させていた送信光パルス発生方式を，連続コヒーレント光を光変調器でパルス化し，これを増幅する方式とした。特に，ミリワットクラスのコヒーレント光を高繰り返しでキロワットクラスの高ピークパワーまで増幅する光増幅器として，非線形効果を用いたパラメトリック光増幅器を新たに開発した。この結果，課題であった送信パルスの繰り返し周波数を大幅に改善し，世界最高となる４kHz(当社従来比200倍)を実現した。一方，送信パルス繰り返し周波数の高速化に伴い，受信信号から風速を算出する信号処理装置の高速化も同時に行った。16個のCPUを用いた並列信号処理装置を新たに開発し，４kHzのパルス繰り返しにリアルタイムで対応可能とした。この結果，距離８キロまでの風速(100メートル間隔)を0.2秒で測定可能な，世界最速となるドップラーライダを実現した。

3. 開 発 結 果

図１に開発したドップラーライダの外観を示す。天井に設けられたスキャナにより，全方位測定が可能である。**図２**に，仰角を固定して方位角を周回走査したときの風速分布の測定結果を示す。風速表示のほかに，風向を含む風速ベクトルでの表示も可能である。また，装置の起動，停止，観測は，すべて，１台のパソコンで制御されており，電話回線によるリモート操作も可能である。

4. ま　と　め

光送信器の高繰り返し化と，信号処理装置の高速度化を図り，風速の三次元分布をリアルタイムで計測可能な波長1.5μm帯のドップラーライダを実現した。この装置は，これまでシミュレーションに頼っていた大気中の細かい気流の構造の時間変化や，乱流の生成から消滅に至る過渡的変化を実測できる新たなツールとして期待できる。今後，この特長を生かした各種応用に適用していく予定である。

図１．リアルタイム風速分布計測ドップラーライダの外観

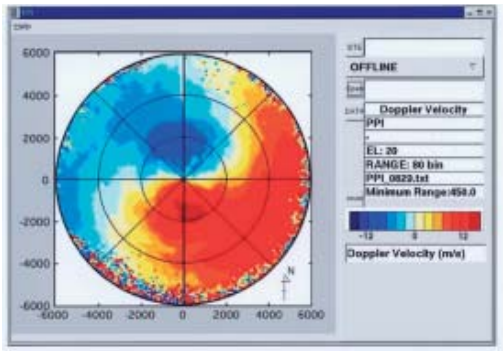
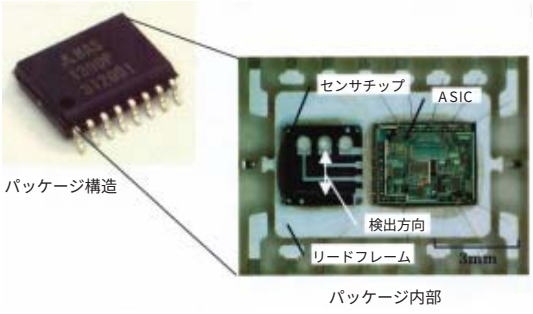


図２．風速分布測定結果例(仰角20°)

高精度MEMS加速度センサ

最新のマイクロマシニング技術であるDRIE(Deep Reactive Ion Etching)プロセスを適用し，高性能加速度センサ(加速度レンジ±２G，G：重力加速度)を開発した。このセンサは，当社従来製品(MAS1370P)と比較して加速度検出精度を２倍にしたほか，オフセット電圧の温度ドリフト量を1/2以下に抑えて検出精度を向上させ，業界最高レベルの小型化と高性能化を実現するとともに，信号処理ICの内蔵により低価格化を図っている。この加速度センサは，液晶プロジェクタの台形補正，カーナビの高度差検出など，様々な民生・産業機器の位置検出制御，傾斜角検出制御，振動制御システムに幅広く適用可能である。



高精度MEMS加速度センサ

携帯電話映像モジュール高機能化技術

携帯電話の競争力アップにはカメラ性能の差別化が重要で，高解像度・高画質化に加えて画像処理時間等使い勝手を決める要素が重要となってきている。そこで，次の映像モジュールの高機能化開発を行った。①PIA(Pixel Interleaved Array)−CCDを用い高感度でSXGA出力画像を得られる小型カメラモジュールの開発，②高フレームレート(20フレーム/秒)かつ遅延の少ないプレビューと高速なJPEG圧縮が可能な映像信号処理ハードウェアモジュールの開発，③高フレームレートを実現する画像転送ソフトウェアや新アルゴリズムを採用したマルチメディア処理ソフトウェアモジュールの開発，④画像評価システム開発を中心とした表示モジュールの開発。

携帯電話映像モジュール高機能化技術

カーナビゲーションの交差点３D表示

間違えやすい交差点も見やすく分かりやすく案内する3D表現を用いた交差点案内表示方法を開発した。

交差点の様々な特徴(アップダウン，立体交差，交差点の連続，合流／分岐の複合等)を交差点の分かりにくさにつながる“複雑さの要因”として分類・整理し，個々の交差点について案内画像の視点と視方向を複雑さの種類や度合いに応じて調整することで，従来は表現しにくかった複雑な形状の交差点も見やすく分かりやすく案内する。

また，案内ルート上のすべての交差点の複雑さを評価し，特に複雑な案内交差点については，案内地点に着く前に，案内交差点の構造を把握しやすい視点からの案内画像をあらかじめ提示して，道誤り防止の効果を高める。

①renzoku，②eikaku，③preView