ICAT NewsLetter Vol,4

認証実用化実験協議会

（財）日本情報処理開発協会内　〒105-0011　東京都港区芝公園3-5-8　☎03-3432-9387

今 号 の 記 事

事 務 局 連 絡

遅れ馳せながら昨年1997年の「RSA Date Security Conference」（RSAカンファレンス）をお送りいたします。

今年のRSAカンファレンスが1998年1月13日から16日まで開催されました（事務局ではレポートを書いてくださる方を探しております）。1998 RSAカンファレンス開催に先立って

1） RSA Challenge II 開催

2） BSAFE4.0で楕円曲線暗号のサポート

がアナウンスされました。2）に関しては１年で世の中の流れが大きく変わったせいであると思われます。

また、年末に 三菱電機の松井氏（暗号技術研究タスクフォース委員）と太田氏がMISTY1 のInternet-draftを出されました。商用利用以外の利用には無償であると明言されています。詳細は

ftp://ds.internic.net/internet-drafts/draft-ohta-misty1desc-00.txt

をご覧ください。　事務局

1997 RSA カンファレンス レポート

報告者：渡辺 晋一郎（アドバンス）
―暗号技術研究タスクフォース委員―

カンファレンス は米国サンフランシスコNob Hillにて、1997年1月28日から1月31日まで開催された。２日目までは、Nob Hillの The Masonic Auditorium 大ホールで行われ、また、その地下では、各メーカーによるデモ展示が行われた。

１．Keynote

RSA社長の挨拶及びカンファレンス会場とワシントンとを衛星中継で結び、政府関係者と暗号、Key Escrow、Key Recoveryについてディスカッションした。（会場からのブーイングもなく）終始穏やかに進行した。政府はKey Escrowの必要性について述べていた。Key Escrow、Key Recoveryについては、プライバシー保護とテロ等の犯罪防止とのトレードオフ等の問題で難しいが、その必要性について今後深く考えていくことになるであろう。

2.General Session

2.1 Cryptographer's Panel

Panelist:　Dr. Peter Neumann（SRI）
Dr. Whit Diffie（Sun）
Dr. Taher ElGamal（Netscape）
Dr. Burt Kaliski（RSA Labs）
Dr. Silvio Micali（MIT）
Dr. Hugo Krwczyk（IBM）
Dr. Ron Rivest（MIT）
Dr. Matt Blaze（AT&T）

現代暗号は、主に第一次世界大戦の時から使用されている。この時代の通信は伝書鳩が使われていた。この小さな伝書鳩が戦争を終了させ、多くの命を救った。鳩は平和のシンボルでもあり（今回のRSAカンファレンスのマスコット？[1)]）、暗号の平和利用を意識していることを強く感じた。

その後、暗号は数学理論を基に作られるようになり、最初の公開鍵暗号は1976年Diffie とHellman（DH暗号）によって考案された。この時Rivestは本当に現実的にできるのかと実現性を疑ったとのこと（笑）。

その後、1977年にRivest、Shamir、AdelmanによってRSAが発表された。この方法は、DHのアイデアをよりよく実現させた方法である。現在ではRSAが多くのところで使用されている。今後さらに応用されたものが発表されるであろう。

2.2 Afternoon Keynote:
RSA, IBM and SecureWay
Kathy Kincaid（IBM）

ネットワークコミュニケーションが主流の現在、情報の秘匿のための暗号化が必要であるが、その暗号化鍵を無くした場合のKey Recoveryの方法も考慮されている必要がある。

また、暗号技術が犯罪に使用された場合、法律的にその暗号化情報にアクセスするためのKey Escrowも必要である。SecureWayはKey RecoveryとKey Escrowの技術の両方を導入している。しかし、その運用はよく考える必要がある。

2.3 Modern InfoSecurity Technology:
The Bigger Picture
John Adams（Security Dynamics）

Security Dynamics社のSecurIDユーザは125万以上、RSADSIの BSAFE ツールキットの配布は８千万コピーである。今、ITマネージャーの心配事は

30%	データ保全
25%	セキュリティ
22%	バックアップツール
22%	システムマネージメントツール
14%	Reduncy

である。セキュリティを向上させるのに必要となる機能は

・強い認証機能
・暗号化機能
・デジタル署名機能
・否認防止
・監査機能

であるとされている。

2.4 Deploying SET:
Bankcards on the Internet
Panelist: Glenn Kramer（Verifone）
Steve Crocker（CyberCash）
Robert Chlebowski
（Wells Fargo Bank）
Willman Powar
（Venture Architects）

SETを広く使用してもらうためには、今後金融の制度改善やルール作りが重要である。これらの仕組みを整えることで、インターネットを利用した電子商取引の利用者が多くなるであろう。

現在考えられている方法は、クレジットカードのカードホルダーがブラウザを使ってSHOPまではSSLで通信し、SHOPからPayment Gateway（与信・決済中継ゲートウェイ）まではSETプロトコルを使用する方法である。

2.5 International Trends in Cryptography
Panelist: Charles Walton（SPYRUS）
Yanping Hu（MOFTEC）
David Naccache（Gemplus）
John Wankmueller（Mastercard）
Hiroyuki Sakubeh（NTT Data）
Ken Mukai（MITI Japan）
Keld Poulsen（Kommunedata）
William Powar
（Venture Architects）

SETを応用したS/PAY、及びRSAを利用したデータベースの紹介が行われた。日本の通産省からはECOM[2]、日本の暗号アルゴリズム、鍵管理技術としてKPS[3]（アドバンス）等が紹介された。

2.6 Cryptography and Information Warfare
Dr.Gerald Kovacich
（Northrop Grumman ）

情報システムへの脅威は、hacker等によるCyber Warが考えられる。これらに対する防衛手段として有効なのは、やはり暗号技術である。しかし、高度な技術に対して旧式な防御手段も有効な場合がある。

2.7 Cryptography's Future:
Opportunities & Threats
Bruce Schneier
（Counterpane Systems）

情報通信に対するアタックが行われるポイントは幾つかある。例えば、通信経路の接続ポイント、端子箱、ケーブル等がある。これらはいつでも無防備であり誰もが侵入できる。このような脅威に対し、暗号ツールが有効なものとなるであろう。しかしながら、さらに攻撃者はその攻撃能力を高めていくので、攻撃を防ぐためにはより強いセキュリティレベルが要求される。

3. CRYPTOGRAPHERS' TRACK

3.1 Recent Trends in the design of Cryptographic Algorithms

Dr.Bart Preneel（Katholieke Univ.）

●ブロック暗号：DES、IDEA、RC5、SAFER

ブロック暗号は、ある鍵を元に平文データを分割した後、シフトレジスタを用いて数bit移動させ、前のデータとXORを計算する方式である。これを何段か行い暗号化する。代表的なブロック暗号であるDESは、古くから様々なアタックがされており、その特徴が分析されている。

また、日本では三菱電機の松井氏がMISTYを２年前に開発したが、まだアタックが十分に行われてきたとは（現時点では）言えず、強度を保証できるところまでには至っていない。

名前	平文ブロック	鍵サイズ	開発元
DES	64bit	58bit、112bit	IBM（米国）
IDEA	64bit	128bit	ascom（スイス）
RC5	64bit	32bit、64bit	RSA（米国）
SAFER	64bit	64bit、128bit	Cylink（米国）

●ストリームサイファ暗号：SEAL、RC4

この方式は、ある大きな乱数列を使用し平文データとXOR等の計算する単純な方式である。しかし乱数列の生成がよければかなり強度の高いものとなる。

3.2 ECDSA ：An Enhanced DSA

Don B. Johnson（Certicom）

・ECDSA[4]とは楕円曲線暗号を使用したDSA[5]である。
・楕円曲線自体は約100年前から考えられている数学である。
・有限体Zp上の楕円曲線の点を求めるのと、その逆計算の難しさを利用している。

keyサイズ（bit）		強度（MIPS年）
RSA/DSA	EC	
512	106	10^4
768	132	10^8
1024	160	10^{12}
2048	211	10^{20}
5120	320	10^{36}

・計算速度が速い。
・よい解読法が確立されていない（強固である）。
  o 160bitまでは、Pohling-Hellman法
  o 1024bitまでは、MOV-reduction法（特定楕円暗号のみ）
・今後、楕円曲線暗号は広く使用されることになるであろう。

4. ANALYSTS' TRACK

4.1 Information Security in the Enterprise

Walt Curts（Entegrity Solutions）

情報セキュリティ事業はここ５、６年で急激に伸びている。しかし今までは使いやすいセキュリティ商品が少なかったため、選択が容易だったと考えられる。今後５、６年はセキュリティ技術も高くなり、選択も難しくなると思われる。今、注目を浴びつつあるのはKey RecoveryやKey Escrowの技術である。今後、様々な会社がこれらの製品を出すであろう。

5. DEVELOPERS' TRACK

5.1 How to Crack a Smartcard

Tom Rowley（National Semiconductor）

●利用にあたっての不安要因
・機能不十分なスマートカード
・供給者の現実回避
・アプリケーション技術の限界

●一般的なアタック方法
・ 旧式機能の利用
・貧弱な構築個所
・ソフトウェア部分攻撃
・ブルートフォース攻撃
・工場の配送ミスの利用

●ROMメモリーへのアタック方法
・直接スマートカードプログラムとアルゴリズムを抜き出す。
・光電子の利用
　赤外線レーザによりチップの中身をスキャニングし、トランジスタ構成の極小電荷と電流を計測する。
・電子ビームスキャニング
　半導体の覆いを剥がし電子ビームを走査する。これによる反射電荷をプローブし、ディスプレィに表示する。

●EEPROM[6]へのアタック方法

EEPROMに保持された電荷を抽出する。電荷はゲートに保持されている。電荷の読み取り方法としては

・チップ内の列線へのアクセス
・スマートカードチップ試験回路の使用
・電子ビームの利用（ROMアタックと同じ方法）

がある。

●今後スマートカードに必要なこと

・セキュアマイコンの開発と使用
・耐タンパー性の強化
・セキュリティモデルの取入れ

6. STANDARD TRACK

6.1 The S/MIME Secure Email Standard

Blake C .Ramsdell（Worldtalk）
Douglas S.Shoupp（Deloitte & Touche）

●PKCS（Public-Key Cryptography Standards）の推奨

PKCS#1	RSA Encryption
PKCS#3	Diffie-Hellman Key Agreement
PKCS#5	Password-Based Encryption
PKCS#6	Extended Certificate Syntax
PKCS#7	Cryptographic Message Syntax
PKCS#8	Private-Key Information Syntax
PKCS#9	Selected Attribute Type
PKCS#10	Certification Request Syntax

●application/x-pkcs7-mime

・暗号化、電子署名の送受信で3種類のデータタイプがある
　o Enveloped Data
　o Signed Data
　o Signed & Enveloped Data
・PEMとの互換性
　PEMはMIME化されていないが PKCS#7に従って暗号化されている。

●application/x-pkcs10

Netscape等のブラウザ同様、証明書の発行要求を行う。

《注釈》

1）**http://www.rsa.com/rsa/conf97/**

2）電子商取引実証推進協議会（Electronic COMmerce promotion council of Japan）。日本情報処理開発協会が事務局を行っている。
http://www.ecom.or.jp/

3）Key Predistribution System（事前鍵配送システム）。横浜国大の松本助教授、東大の今井教授が1986年に考案した鍵配送アルゴリズム。

4）Elliptic Curve analog of the Digital Signature Algorithm。楕円曲線上のDSA。

5）Digital Signature Algorithm。離散対数問題の困難性をベースにした署名方式。NIST（米国標準技術院）によって米国連邦情報処理標準（Federal Information Processing Standard）FIPS PUB 186に定められている。米国政府が特許を所有している。

6）Electrically Erasable Programmable Read-Only Memory。電気的に消去（書き換え）できるROM。

事務局連絡

ー1998年2月4日（水）定例研究会延期についてー

誠に申し訳ありませんが、前号のNewsletterでアナウンスいたしました 定例研究会 を都合により延期とさせていただくことになりました。

次回の開催は4月初旬を予定しておりますが、今のところ未定です。詳細が決まり次第ご連絡いたしますのでご了承ください。

なお、次回の定例研究会では平成9年度の活動報告を中心としたプログラムを計画しております。今年度ICATでは

（1） 代行認証機能
（2） 階層構造での認証局機能
（3） 汎用暗号ライブラリー
（4） PKIコストモデル
（5） 認証局運営規定

の開発・作成を行っております。当日のプログラムといたしまして、（1）～（3）についてそれぞれの開発者から発表する予定でおります。