CRYPTO2000 出張報告

（2000.10.2 修正版）

IPA セキュリティセンター
暗号技術調査室　山岸篤弘

1.目的

平成１２年度「暗号技術調査室」調査・情報収集活動の一環として、国際的な暗号学会である Crypto2000 に参加した。

2.CRYPTO2000 状況

今回の CRYPTO2000 には、３５カ国４５２名の参加者があった。うち、日本からは２６名が参加していた。国別の内訳、日本の企業別参加者の内訳は別表を参照。招待講演２件とランプセッションを含め、１５のセッション(３２件)が構成された。

2.1 XTR and NTRU

- **The XTR public key system (Lenstra, Verheul)**
- **A chosen ciphertext attack against NTRU (Jaulmes, Joux)**

上記の２件の発表があり、前者は DSA への実装を意識した新しい方式が提案された。後者は、NTRU への選択暗号文攻撃の結果報告である。

新しい方式の提案であっても、安全性に関する自己評価が行われており、RSA 暗号や ECC 暗号との比較がなされていた。自己評価についても、学術的にしっかりとした裏付けをとっていることは当然というものの我が国との違いを痛感する。

2.2 Privacy for database

- **Privacy preserving data mining (Lindell, Pinkas)**
- **Reducing the servers computation in private information retrieval (Beimel, Ishai)**

上記の２件の発表があった。”Privacy preserving data mining” は、データ・マイニングの分野で、ZKIP (Zero-Knowledge Interactive Proof) と似た手法を使い、ベスト・アトリビュートを計算することで、データベース中のプライバシー情報を外部に漏らさないシステムが構築できることを示した。

2.3 Invited talk(The development of DES)

第１日目で、最も興味深い講演は、米国標準暗号 DES の開発者である Coppersmith (IBM)による招待講演 ”The development of DES” であった。米国標準暗号 DES は、現在選考が進められている AES と同様、1973 年、1974 年に行われた NIST(当時は NBS)の公募プロジェクトに米国 IBM 社が応募した暗号である。

DES の原型になった暗号は、”Lucifer” と呼ばれる暗号方式であり、ブロック長 32bit、鍵長 128bit のブロック暗号であるという。構造的には、”Invertible”であり、S-box の構造も DES とは異なり、4bit 入力 4bit 出力である。この”Lucifer”の S-Box は 4bit 入力がそれぞれ独立であるが、この S-Box の構造を、「隣接する S-Box と影響させる」様に変更した、すなわち、隣接する S-Box の入力 1bit ずつを加え、6bit 入力 4bit 出力に変更し、非可逆(Non-invertible)に変更したものが DES の基本構造となっている。また、DES では “Fesitel Ladder” 構造が採用され、その構造上、差分解読確率 p(Δout=0｜Δin)＞0 となるため、差分解読法 “Differential Cryptanalysis” に対する考慮が考慮されたという。つまり、Shamir, Biham により差分解読法が明らかにされるよりも以前に、差分解読法という評価技術が存在していたということである。この情報は、松井充氏(三菱電機)が CRYPTO94 で報告した S-box の並びが、差分解読法に対して「強い並び」となっているという発見で裏付けられている。

DES の開発に係わった米国 IBM 社の関係者は、Alan Kenheim, Ray Adler, Bill Nutz, Lynn Smith, Horst Fesitel, Alan Tritler, Bryant Tuckerman, Carl Meyer, Edna Grossman, Bob McNeill, Walt Tuchmann, Jon Oseai, Don Coppersmith の１４名であったという。

講演後の質疑の中で、NSA の関与を質問されたが、「鍵サイズの変更」が主であったとのことであり、「なぜ、56bit か？」との問いに対し、「NSA が、”Perfect Number”と思ったのであろう。」はぐらかした回答があった。また、S-Box の設計基準に対しても、差分解読法に対する数学的根拠が示された。

2.4 Secure distributed computation and applications

- **Parallel reducibility for information-theoretically secure computation(Yevgeniy Dobis, Silvio Micali)**
- **Optimistic fair secure computation(Christian Cachin, Jan Camenisch)**
- **A cryptographic solution to a game theoretic problem(Yevgeniy Dobis, Shai Halevi, Tal Rabin)**

上記の３件の講演があった。分散計算環境下で、各サーバー上でも情報を他者に漏らさない様に処理を実施するためのプロトコルの検討。日本では、まだ分散環境下でセキュリティに関する研究者の層が薄いが、今後発展すると思われる分野である。

2.5 Algebraic Cryptosystems

- **Differential fault attacks on elliptic curve cryptosystems(Ingrid Biehl, Bernd Meyer, Volker Mueller)**
- **Quantum public-key cryptosystems(Tatsuaki Okamoto, Keisuke Tanaka, Shigenori Uchiyama)**
- **New Public-key cryptosystem using groups(Sangjin Lee, Jung Hee, Jaewoo Han, Ju-sung Kang)**

最初の１件目は、楕円暗号(ECC)を実装する際に考慮すべき差分故障解析に関する検討。RSA 暗号の差分故障解析を拡張している。

２件目は､計算量理論に安全性の根拠を有する暗号方式(RSA 暗号や楕円暗号)の次の世代の公開鍵暗号系に対する提案。基本コンセプトレベル？

３件目は、「組み糸群(Braid group)」を用いた公開鍵暗号系の提案。慶応大 SFC 武藤教授の博士論文で提案された暗号や金沢大林先生の「ラティス暗号」の親戚。安全性の評価を３種類の攻撃法につき検討している。

2.6 Message Authentication

- **Key recovery and forgery attacks on the macdes mac algorithm(Don Coopersmith, Lars Kundsen, Chris Mitchell)**
- **CBC macs for arbitrary-length messages: the three-key constructions(John Black, Phillip Rogaway)**
- **L-collision attacks against randomized macs(Michael Semanko)**

３件とも MAC に関する安全性評価。

１件目は、講演者が提案した DES ベースの MAC で、鍵の推定や MAC の偽造が可能性を指摘した。

２件目は、任意データ長の情報に対するブロック暗号の CBC モードベースの MAC(ECBC,FCBC,XCBC)の安全性評価。

３件目は、ランダマイズ MAC に対する安全性評価。MAC 情報と対象の情報を格子状に並べると３つの格子点(丁度「L」字型になる)が決まると残りの１点が推定でき、偽造が可能となると指摘している。このような場合が生じるのは、64bit ブロック暗号であれば、2^{43} 個のタグ情報が必要であり、128bit ブロック暗号であれば、2^{86} 個のタグ情報が必要であると見積もっている。今年 10 月 20 日に、NIST が主催する「Symmetric Key Block Cipher Modes of Operation Workshop」への貢献目的か？

2.7 Digital signatures(デジタル署名)

- **On the exact security of Full-Domain-Hash(Jean-Sebastien Coron)**
- **Timed commitments(Dan Boneh, Moni Naor)**
- **A practical and provably secure coalition-resistant group signature**

scheme(Giuseppe Ateniese, Jan Camenisch, Marc Joye, Gene Tsudik)

- **Puruvable secure partially blind signatures(Masayuki Abe, Tatsuaki Okamoto)**

デジタル署名に関しては、４件の講演があった。１件目は、FDH(Full-Domain-Hash)に関する安全性の証明法の改良を提案している。２件目は、時限付き commitment(プロトコル)の提案。RSA 暗号や Rabin 暗号を用いて実現している。３件目は、企業体等での使用を想定したグループ署名法(プロトコル)の提案。４件目は、ユーザー(署名者)の不正を防ぐため、一部の情報を開示するブラインド署名法(プロトコル)の提案。一般のブラインド署名は封筒の上から署名することに相当するが、提案方式は、窓付きの封筒で窓から、署名対象情報の一部が観測でき、署名者がだまされる可能性を減少させている。

2.8 Ramp session

ランプセッションは３部構成で、１発表あたり最大 10 分程度の極めて限定された発表であった。発表件数は、３２件(総発表時間は２時間強)。AES に関する報告は、Foti ではなく、Morris Dworkin が行った。発表内容は、極めて「公式的な」内容であり、ブーイングとヤジで発表者は苦笑していた。ヤジの内容は、「教科書的な内容は良いから、どの finalists が AES として選定されるんだ！早く言って楽になったら？」と半分からかうような内容であり、聴衆から大きな歓声と拍手を浴びていた。

2.9 Cryptanalysis

- **Weakness in the $SL_2(F_{2^n})$ hashing scheme(Rainer Steinwandt, Markus Grassl, Willi Geiselman, Thomas Beth)**
- **Fast correlation attacks through reconstruction of linear polynomials(Thomas Johansson, Fredrik Jonsson)**

暗号解読に関しては、２件のみ。ひとつは、特殊線形群 SL_2(F_{2^n})をベースとしたハッシュ関数に対する新しい「弱点」の報告。パラメータによっては「トラップドア」ができてしまうことが指摘された。ストリーム暗号に対する“一般的な”攻撃である。学習理論を応用し、”Fast correlation attack” を達成している。類似の方法として、遺伝アルゴリズム(GA)を用いた方法が提案されたことがあり、比較検討が必要と考える。

2.10 Traitor tracing and broadcast encryption

- **Sequential traitor tracing(Reihaneh Safavi-Naini, Y. Wang)**
- **Long-lived broadcast encryption(Juan Garay, Jessica Staddon, Avishai Wool)**

今回の CRYPTO では、最も応用よりのセッションであった。放送系での暗号の応用がテーマ。

１件目の発表は、放送系を用いた暗号通信路で、不正者を割り出す手法の提案。基本的なアイデアは、ユーザーをセグメントに分割し、この割り当てを準動的に変更する。この

とき、不正者の属するセグメントに関する情報を収集することで、不正者を特定しようとしている。計算量がかなり大きく、局間中継でしか使えないのではないかと思われる。

２件目の発表は、長寿命の放送用暗号系の構成に関する提案。聴取カードに対する攻撃を受けても、被害を限定しカード再配布の発生を軽減している。この方式の効果をモデルによるシミュレーションで確認している。

2.11 Invited talk(Taming the adversary : Martin Adabi)

暗号系を形式的に評価する手法を紹介している。現行の情報セキュリティ・システムにおける暗号技術の適用とその評価は、かなりヒューリスティックな部分が多いが、暗号操作を形式的(formal)に記述することで、形式的な安全性が評価できるとしている。ケルベロス(Kerberos)の場合をモデルに検討されていた。発表者はこの研究で ACM の表彰を受けた様である。

2.12 Symmetric encryption(共通鍵暗号)

- **The security of All-Or-Nothing Encryption : Protecting against Exhaustive Key Serach(Anand Desai)**
- **On the round security of symmetric-key cryptographic primitives(Zulfikar Ramzan, Leonid Reyzin)**
- **New paradigms for constructing symmetric encryption schemes secure against chosen ciphertext attack(Anand Desai)**

共通鍵暗号系の発表は、３件。

１件目は、ブロック暗号の新しいオペレーションモード”All-or-Noting transfer(AONT)”に関する内容である。”All-or-Noting transfer”は FSE97 で Rivest により提案された。この発表では、ブロック暗号により構成された AONT のシャノン・モデルにおける安全性の証明を行っている。

２件目は、Luby-Rackoff 流のブロック暗号を構成したときの安全性評価である。この方法は、MAC やユニバーサルハッシュ関数でも適用できると主張している。

３件目は、選択暗号文攻撃に対抗できる共通鍵暗号方式の構成法の提案である。

2.13 Commit or not commit

- **Efficient non-malleable commitment schemes(Marc Fischlin, Roger Fishlin)**
- **Improved non-committing encryption schemes based on a general complexity assumption(Ivan Damgard, Jesper Buus Nielsen)**

１件目の発表は、従来の non-malleable commitment の手法に、ZKIP の考え方を適用し、安全性を高めた方式の提案。

２件目は、シミュレート可能な non-committing encryption schemes の改良。

2.14 Protocols(プロトコル)

- **A note on the round-complexity of concurrent zero-knowledge(Alon Rosen)**
- **An improved pseudo-random generator based on discrete log(Rosario Gennaro)**
- **Linking classical and quantum key agreement : is there "bound information"?(Nicolas Grisin, Stefan Wolf)**

1件目は、仮定なしで8回の交信で ZKIP **が実現できると主張している。更新回数の下限を改良している。**

2件目は、Blum-Micall **の** PRBG **の改良。3件目は、従来の鍵共有方式と量子暗号鍵共有方式とを、情報量を利用して関係付けている。**

2.15 Stream cipher and Boolean functions

- **Maximum correlation analysis of nonlinear s-boxes in stream ciphers(Muxiang Zhang, Anges Chan)**
- **Nonlinearity bounds and constructions of resilient Boolean functions(Palash Sarkar, Subhamoy Maitra)**
- **Almost independent and weakly biased arrays: efficient constructions and cryptologic applications(Juergen Bierbrauer, Holger Schellwat)**

1件目は、ストリーム暗号における非線形 S-Box **の安全性評価を行っている。複数の** LFSR(Linear Feedback Shift Registers)**を用いてストリーム暗号を実現する方法は、大まかに** Filter **型と** Combination **型が存在するが、**Filter **型の方式で、**Filter **部を** S-BOX **で代替すると、処理速度は速いが、情報が漏れると主張している。**

2件目、3件目は、(共通鍵)暗号の基本構成要素であるブール関数の性質に関する内容である。ブール関数は、暗号には重要な構成要素であるが、だんだん純粋数学に近い内容となっている。

3 その他(IEEE Koji Kobayashi Computers and Communications Award)

1999 年度及び 2000 年度の IEEE 小林宏治記念賞受賞者の表彰式が第１日目(８／２１午後)行われた。

1999 年度受賞者は、Martin E. Hellman(スタンフォード大), Whitfield Diffie(サン), Ralph C. Merkle(Zyvex)の３名。受賞理由は、「公開鍵暗号原理の創出」。

2000 年度の受賞者は、Ronald L. Rivest(MIT), Adi Shamir(Weizmann Institute of Science), Leonard Adleman(MIT)の３名。受賞理由は、「RSA 暗号方式の発明とその実用化」。授賞式後の挨拶の中で、Hellman 教授が、公開鍵暗号原理、RSA 暗号を最初に発見した英国 GCHQ の業績にふれていたのが印象的であった。

4 所感

発表全体の傾向は、関連の学会(EUROCRYPT、ASIACRYPT、FSE、SAC、CHES、PKC、ECC 等)が増えたこともあり、また、CRYPTO の採択率が、30%前後と極めて厳しいため、だんだんと専門化(狭隘化)が進み、CRYPTO だけを見ていれば、全体の状況がつかめるというわけには行かなくなってきている。発表も公開鍵暗号プリミティブを利用したスキーム(プロトコル)に関する発表が主力であり、この分野では、日本からの発表が少ない(１件)のが残念である。参加者の話では、先進的な内容は EUROCRYPT の方が多い(査読が緩い)ということであった。

参加者の傾向は、後掲の表を見てもわかるとおり、米国は別として、仏、独、韓国、日本、加からの参加者がほぼ同数であった。特に目を引くのが韓国からの参加者の増加であり、韓国が暗号をはじめとして情報セキュリティ分野での研究開発に力を注ぎはじめたとの印象が強い。

5 修正履歴

2.9 Cryptanalysis を修正。（2000.10.2）

別表

国名	人数
米国	200
日本	26
カナダ	21
サウジアラビア	2
シンガポール	3
韓国	28
ハンガリー	1
フランス	29
ドイツ	28
イスラエル	9
デンマーク	4
英国	15
スウェーデン	10
ベルギー	5
スイス	8
中国(台湾)	7
アルゼンチン	3
中国(本土)	3
イタリア	2
オーストラリア	7
クロアチア	2
ブラジル	4
オランダ	7
ルーマニア	4
フィンランド	8
アイルランド	1
スロバキア	3
ノルウェー	4
チェコ	1
スロベニア	1
ロシア	1
ペルー	1
南アフリカ	2
ポーランド	1
ニュージーランド	1
合計	452