EUROCRYPT 2003 会議報告

盛合　志帆[†]　大塚　玲[‡]　今井　秀樹[*]

†ソニー・コンピュータエンタテインメント　〒107-0062 東京都港区南青山 2-6-21
‡IPA セキュリティセンター　〒113-6591 東京都文京区本駒込 2-28-8
*東京大学 生産技術研究所　〒153-8505 東京都目黒区駒場 4-6-1
E-mail:　†shiho@rd.scei.sony.co.jp,　‡a-otsuka@ipa.go.jp,　*imai@iis.u-tokyo.ac.jp

あらまし　2003 年 5 月にポーランド・ワルシャワで開催された、国際暗号学会 IACR (International Association for Cryptologic Research) 主催の国際会議 EUROCRYPT 2003 について報告する.
キーワード　EUROCRYPT 2003, 国際暗号学会

EUROCRYPT 2003 Report

Shiho MORIAI[†]　Akira OTSUKA[‡]　and　Hideki IMAI[‡]

† Sony Computer Entertainment Inc.　2-6-21 Minami Aoyama, Minato-ku, Tokyo, 107-0062 Japan
‡ IT Security Center, IPA　2-28-8 Honkomagome, Bunkyo-ku, Tokyo, 113-6951 Japan
* Institute of Industrial Science, the University of Tokyo　4-6-1 Komaba, Meguro-ku, Tokyo, 153-8505 Japan
E-mail:　†shiho@rd.scei.sony.co.jp,　‡a-otsuka@ipa.go.jp,　*imai@iis.u-tokyo.ac.jp

Abstract　This paper reports on EUROCRYPT 2003, sponsored by the IACR, the International Association for Cryptologic Research. This conference was held in Warsaw, Poland, in May, 2003.
Keyword　EUROCRYPT 2003, IACR

1. 会議の概要

EUROCRYPT 2003 は今年で 22 回目を迎え、2003 年 5 月 4 日～8 日にポーランドの首都ワルシャワにて開催された。開催場所はワルシャワ中央駅の前にそびえる文化科学宮殿 (Palace of Culture and Science)（図 1 参照）であった。参加者は 357 名と例年の会議に比べて少なめで、国別参加数の多い順に USA 46 名、ポーランド 45 名、フランス 42 名、ドイツ 32 名、イギリス 22 名、ベルギー、スイス 16 名… となっていた。韓国 6 名、日本 4 名、台湾 4 名と、SARS の影響を受けてか、アジア地域からの参加者は少なかった。

プログラムについては、156 件の投稿論文中から 37 件の論文が受理され、14 のレギュラーセッションでそれぞれ発表された。招待講演では、「初めて Enigma を破った国」*"the country of people who broke the Enigma"* ポーランドでの開催にちなんで Arkadiusz Orlowski により"Facts and Myths of Enigma: Breaking Stereotypes" という演題で Enigma の解読をめぐる歴史について紹介された。Enigma 実機も壇上に登場し、大変興味深い講演であった。もう 1 件の招待講演は Jacques Stern による"Why Provable Security Matters" という講演で、暗号の証明可能安全性とは何か、また注意すべき点は何かについて実例を交えながら話された。また、例年通り、リラックスしたムードの中、アナウンスや最新の成果についてのショートプレゼンテーションが行われる Rump セッションでは Stanislaw Jarecki による司会で 30 件の発表があった。

図 1　文化科学宮殿

2. プログラム

2.1. Cryptanalysis I (chair: *Serge Vaudenay*)

Cryptanalysis of the EMD Mode of Operation (*Antoine Joux*)

本論文では2002年にRogawayによって提案されたdisc-sector暗号方式EMD (Encrypt-Mask-Decrypt)の安全性について述べられている。EMDはnビットブロック暗号を利用してnmビットブロック単位（ディスクのセクタサイズに対応）での暗号化を行う暗号利用モードと見ることができ、CRYPTO2002でLiskov, Rivest, Wagnerにより提案されたtweakable block cipherの概念が利用されている。本論文では、EMDの攻撃例を示し、安全なtweakable block cipherでないことが示された。EMDと同時に提案された並列化可能なバージョンEMEも同様に攻撃可能である。EMDを修正したアルゴリズムはCRYPTO2003で発表される。

On the Optimality of Linear, Differential and Sequential Distinguishers (*Pascal Junod*)

統計的仮説検定(statistical hypothesis testing)の理論と概念を、線形攻撃や差分攻撃における鍵推定でのlinear distinguisher, differential distinguisherの漸近的な解析に適用し、鍵推定に必要な既知平文数や選択平文数のboundを改良した。また、著者は最初のブロック暗号の統計的解析はDavis-MurphyのDES攻撃に遡るとし、その攻撃で用いられている概念をsequential distinguisherとして定式化し、その有意性を示した。

A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms (*Alex Biryukov, Christophe De Canniere, An Braeken, Bart Preneel*)

ブロック暗号の解析では、線形特性や差分特性など、線形変換やアフィン変換により不変な特性を利用することがある。本論文では任意の2つのpermutation (S-box)が線形(アフィン)等価か判定する効率のよいアルゴリズムを示した。具体的には、2つの$n \times n$-bit permutationの線形等価性 (linear equivalence)を$O(n^3 2^n)$の計算量で判定するアルゴリズムと、アフィン等価性(affine equivalence)を$O(n^3 2^{2n})$の計算量で判定するアルゴリズムを示した。これを用いてRijndael, DES, Camellia, Misty, Kasumiなどの暗号の等価表現を見つけている。

2.2. Secure Multi-Party Computation I (chair: *Berry Schoenmakers*)

Two-Threshold Broadcast and Detectable Multi-Party Computation (*Matthias Fitzi, Martin Hirt, Thomas Holenstein, Jurg Wullschleger*)

Eurocrypt'02で発表されたFitziらのDetectable Broadcastを拡張し、2つの閾値を持つBroadcastとMultiparty Computationの構成法を示している．2つの閾値t, T ($t \leqq T$)と、悪意のある利用者の数fに対して、(1) $0 \leqq f < t$ の場合は通常のSecurity要求を満たすBroadcastおよびMultiparty Computationを実現できるが、(2) $t \leqq f < T$ の場合は、BroadcastがValidityかConsistencyのいずれか一方のみを満たす．このBroadcastを用いて、全てのプレイヤーが正しい出力をするか、全員が一斉にAbortできるようなDetectable Multiparty Computationが構成できることが示されている．

Fair Secure Two-Party Computation (*Benny Pinkas*)

著者らは、CRYPTO2000で発表されたBoneh-NaorのTimed-Commitmentに基づき、commitmentから秘密を求めるのに要する時間が、ヒントを交換する度に半分になるGradual Release Timed-Commitmentを提案し、これを用いて任意のSecure Two-Party ComputationをFairなSecure Two-Party Computationに変換するコンパイラの構成法を示している．提案手法は、Multiparty Computationに前処理と後処理の形で追加されるため、Multiparty Computationの構成と独立であり、Gate毎効率も良い．

On the Limitations of Universally Composable Two-Party Computation without Set-up Assumptions (*Ran Canetti, Eyal Kushilevitz, Yehuda Lindell*)

いかなるSet-up assumption (common reference stringの存在等)も仮定しない条件の下で、Two-party ComputationがUniversal Composabilityを満たすために、関数に求められる条件について述べている．著者らは関数を決定的な場合と確率的な場合に分け、それぞれの必要十分条件と十分条件を示している．

2.3. Invited Talk I (chair: *Andy Clark*)

Facts and Myths of Enigma: Breaking Stereotypes (*Arkadiusz Orlowski, Kris Gaj*)

Arkadiusz Orlowski が Enigma の歴史やそのしくみ、いかにポーランド人数学者が Enigma の解読に貢献したか、そして Enigma 解読から得るべき教訓について話された。Enigma が Alan Turing 率いる英国チームによって解読されたことは有名であるが、第 2 次世界大戦前にポーランド人数学者 Marian Rejewski が進めていた解析情報の功績が大きかったという。講演中、壇上には Enigma 実機が展示され、会場を大いに沸かせた。

2.4. Zero-Knowledge Protocols (chair: *Yevgeniy Dodis*)

Resettable Zero-Knowledge in the Weak Public-Key Model (*Yunlei Zhao, Xiaotie Deng, C. H. Lee, Hong Zhu*)

Canetti, Killian, Petrank, Rosen らによって提案された BPK (Bare Public-Key) モデルにおいては, rZK (resettable Zero Knowledge) が concurrent soundness を満たすことが必ずしも保証されない. BPK の制約を強めた Micali, Reyzin らによる UPK (upper-bounded public-key)においては rZK が concurrent soundness を満たすことを保証できる. 著者らは, BPK と UPK の中間に位置する WPK (Weak Public-Key)モデルを提案し, WPK モデルにおいても rZK の concurrent soundness が保証されると主張している.

Simulatable Commitments and Efficient Concurrent Zero-Knowledge (*Daniele Micciancio, Erez Petrank*)

著者らは Public coin honest verifier ZKP を持つようないかなる言語からも, 不正な verifier を許す concurrent ZKP プロトコルが PKI 等を仮定しない standard model の下で構成できることを主張している. 帰着の際に simulatable commitment というプリミティブを導入することで効率が高まり, セキュリティパラメータ n に対して round complexity と computational complexity を, 元の ZKP の複雑さとは独立に, それぞれ $\omega(\log n)$でおさえられる.

Simulation in Quasi-polynomial Time, and its Application to Protocol Composition (*Rafael Pass*)

著者らは Simulator の実行時間の上限を多項式時間から $n^{\mathrm{poly}(\log n)}$に緩和することで, concurrent 実行環境の下での ZKP の安全性証明を plain model で (common reference string なしに)与えられると主張している.

Strengthening Zero-Knowledge Protocols Using Signatures (*Juan Garay, Phil MacKenzie, Ke Yang*)

EUF-ACMA 署名と common reference string モデルを仮定すれば, いかなる honest Verifier ZKP も concurrent, unbounded simulation sound, non-malleable かつ universally composable な ZKP の下で変換できると主張している.

2.5. Foundations and Complexity Theoretic Security (chair: *Nigel Smart*)

Nearly One-Sided Tests and the Goldreich-Levin Predicate (*Gustav Hast*)

Goldreich-Levin ハードコアビットを $1/2+\varepsilon$ の確率で予測する adversary $\mathcal{A}$ が存在すると, 最も効率の良い Adcock-Cleve の方法では確率 ε^2 で逆関数を求められる. 著者らは 0, 1 の出力に偏りがあり, 判定できない場合に $\perp$ の出力も許す Nearly One-sided Test を考えると, ε^2/p の確率で効率良く逆関数を求められると主張している. ここで p は Test が 0 か 1 を出力する確率である. このことを利用して帰着効率の高い Blum-Micali 疑似乱数生成器が構成できることが示されている.

Efficient and Non-Malleable Proofs of Plaintext Knowledge and Applications (*Jonathan Katz*)

Aumann-Rabin が 2000 年に発表したマニュスクリプトで提案された Proof of Plaintext Knowledge(暗号文に対応する平文の知識を証明) に関する発表である. 著者は, 特定の数論的仮定をおくことで効率を高め, non-malleability を満たし, 不正な検証者に対しても安全で, concurrent composition の環境下でも安全性の証明が可能なスキームを構成できると主張している.

2.6. Public Key Encryption (chair: *David Pointcheval*)

A Public Key Encryption Scheme Based on the Polynomial Reconstruction Problem (*Daniel Augot, Matthieu Finiasz*)

Polynomial Reconstruction problem (PR) とは、$n, k, t, (x_i, y_i)$ $(i=1 \ldots n)$が与えられたとき、deg $p(X) < k$ で、かつ、少なくとも t 点で $p(x_i)=y_i$ が成り立つような多項式 $p(X)$ を出力する問題である。PR は 1999 年に新しい「困難

な問題」として紹介されて以来、これに基づくいくつかの暗号プリミティブが設計されてきた。例えばNaorとPinkasにより oblivious polynomial evaluation の構成に応用されたり、Kiayias と Yung により semantically secure な共通鍵暗号に応用されてきている。本論文ではこの問題の困難性に基づく初めての公開鍵暗号方式が提案されたが、rump session でこれを解読する方法がCoronとKiayias-Yungから独立に発表された。

A Simpler Construction of CCA2-Secure Public-Key Encryption under General Assumptions (*Yehuda Lindell*)

trapdoor permutation の存在を仮定した CCA2 (adaptive chosen ciphertext security)を達成する公開鍵暗号スキームのより簡単な構成法が示された。従来のSahaiやDe Santisらの公開鍵暗号スキームに比べてよりシンプルな点がポイントである。この論文の技術的な貢献はシンプルな one-time simulation-sound NIZK (Non-Interactive Zero-Knowledge proof)を構成した点である。

A Forward-Secure Public-Key Encryption Scheme (*Ran Canetti, Shai Halevi, Jonathan Katz*)

暗号処理はしばしば必ずしも安全でないデバイスで実行されることがあり、そこから鍵が暴かれることは深刻かつ現実的な問題である。forward-secure スキームは、秘密鍵が定期的に更新され、万一鍵が暴かれてもその時点より前の情報は安全に保たれる方式である。これまで多くの forward-secure なディジタル署名、鍵交換プロトコル、共通鍵暗号スキームが提案されているが、本論文で提案されたのは、最初の non-interactive forward-secure 公開鍵暗号スキームであり、BTE (Binary Tree Encryption)という新しいプリミティブを使って構成されている。安全性については standard model で決定的 bilinear Diffie-Hellman 問題の困難性を仮定して証明がなされている。

Certificate-Based Encryption and the Certificate Revocation Problem (*Craig Gentry*)

本論文では公開鍵証明書(certificate)ベース暗号方式が提案された。このモデルでは、公開鍵証明書(署名)が公開鍵証明書としての役割だけでなく、復号鍵として機能する。あるメッセージを復号するためには秘密鍵と最新の公開鍵証明書が必要となる。この方式では公開鍵証明書無効化に伴って発生する third-party query をなくすことができるため、従来より少ないコストのインフラで効率のよいPKIの構築が可能となる。

2.7. New Primitives (chair: *Helena Handschuh*)

CAPTCHA: Using Hard AI Problems for Security (*Luis von Ahn, Manuel Blum, Nicholas Hopper, John Langford*)

CAPTCHA は、人間なら簡単に解けるが、現在のコンピュータでは難しい問題を生成して採点する自動プログラムである。例えば、図2に示すようなゆがんだ文字は、人間なら読めるが、現在のコンピュータでは難しい。本論文では、この「困難な問題」をセキュリティに利用する方法が紹介されている。

図2：CAPTCHA (http://www.captcha.netより)

Concealment and its Applications to Authenticated Encryption (*Yevgeniy Dodis and Jee Hea An*)

本論文では concealment という新しい暗号プリミティブを提案し、メッセージ認証付暗号化(Authenticated Encryption)への応用を提案している。

2.8. Cryptanalysis II (chair: *Lars Knudsen*)

Predicting the Shrinking Generator with Fixed Connections (*Patrik Ekdahl, Willi Meier, Thomas Johansson*)

Shrinking Generator (SG)は 1993 年に Coppersmith, Krawczyk, Mansour により提案された擬似乱数生成器である。本論文ではSGに対する実用的な distinguishing attack が提案されている。この攻撃は LFSR を生成する feedback polynomial の既知で重みが低い場合に適用可能で、例えば 2^{32} ビットの出力から、重み 4、次数 10000 もの多項式を利用した SG を識別することができる。

Algebraic Attacks on Stream Ciphers with Linear Feedback (*Nicolas T. Courtois, Willi Meier*)

AES 等に適用されている著者らの代数的攻撃法をstream暗号に応用したもの。この手法は ICISC'02 にて最初に発表され、日本電子政府暗号評価プロジェクト CRYPTREC に提案されていた TOYOCRYPT に適用さ

れ、2^{92} CPU clock で解読できることが示されていた。本論文ではさらに overdefined な連立代数方程式を解く方法を工夫し、2^{49} CPU clock で 20K バイトの鍵ストリームから解読できるようになった。この方法は EU 暗号評価プロジェクト NESSIE に提案されていた LILI-128 にも適用され、2^{57} CPU clock で解読に成功している。

2.9. Elliptic Curves Cryptography (chair: *Luis Granboulan*)

Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time (*Reynald Lercier, David Lubicz*)

本論文では楕円曲線上の有理点の個数を $O(n^{2+\varepsilon})$の計算量でカウントするアルゴリズムが示された。この計算量は Gaussian Normal Basis をもつ有限体の場合に達成される。より一般的には Vercauteren のアイデアを用いれば、事前計算なしで $O(n^{2.69+\varepsilon}\log n)$ビット演算の時間計算量と $O(n^{2.5})$のスペースで計算できるアルゴリズムとなる。また、このアルゴリズムは従来アルゴリズムよりも実装の観点からも容易であろうと主張されている。

The GHS Attack Revisited (*Florian Hess*)

GHS (Gaudry-Hess-Smart) 攻撃の Weil descent construction を任意の Artin-Schreier extension に一般化し、より多くの曲線に適用可能とした。基本の GHS 法で攻撃可能な曲線の数はほぼ 2 乗となり、$\mathbf{F}_2^{155}$ 上の曲線の強度がさらに弱くなった。また、GHS 法の他の extension や variation についても検討されているが、さらなる改良は難しそうであるとの結論である。なお、この攻撃は $\mathbf{F}_p$ 上の曲線には適用できない。

Improved Algorithms for Efficient Arithmetic on Elliptic Curves Using Fast Endomorphisms (*Mathieu Ciet, Tanja Lange, Francesco Sica, Jean-Jacques Quisquater*)

多くの楕円曲線上のアルゴリズムにおいて最も計算量を必要とするのがスカラー倍の計算である。本論文では、CRYPTO'97 で発表された Solinas のアプローチと同程度の速度でスカラー倍の計算を実行できるよう、Koblitz curve の τ 進展開を、高速に計算できる自己同型写像 ϕ をもつ素体上の曲線に適用する手法について示している。具体的には、Solinas の Joint Sparse Form に倣って、ϕ 進展開の利点と Joint Sparse Form による速度向上を併せもつ ϕ - Joint Sparse Form を導入した。

2.10. Digital Signatures (chair: *Shiho Moriai*)

A Signature Scheme as Secure as the Diffie-Hellman Problem (*Eu-Jin Goh, Stanislaw Jarecki*)

帰着効率が悪い署名では、署名の偽造の困難さを 2^{80} 程度に保つためには、基になる問題のサイズを大きくする必要がある. 例えば Pointcheval と Stern の Forking Lemma を用いた証明では Schnorr 署名から離散対数問題への帰着効率は 2 乗に比例するため, 2^{160} 程度の困難さを離散対数問題に持たせる必要がある. 著者らは, CDH に基づき, ランダムオラクルモデルの下で帰着効率が線形な署名方式を提案している. 同じ安全性条件の下では提案方式は Schnorr 署名より効率が良い.

Aggregate and Verifiably Encrypted Signatures from Bilinear Maps (*Dan Boneh, Craig Gentry, Ben Lynn, Hovav Shacham*)

著者らによって CRYPTO2001 で発表された GDH に基づく署名方式を発展させ, Bilinear マッピングを用いた Aggregate signature と Verifiably Encrypted Signature を提案している.

Hypercubic Lattice Reduction and Analysis of GGH and NTRU Signatures (*Michael Szydlo*)

GGH と NTRUSign については, 数千個の署名を受け取った後に秘密鍵を求める問題が, Gram Matrix Factorization Problem と等価であるとして, 著者らはこの問題が比較的易しいと考えられる Lattice Distinguish Problem に多項式時間に帰着できるため, 破れる可能性が高いと主張している.

2.11. Invited Talk II (chair: *Moti Yung*)

Why Provable Security Matters? (*Jacques Stern*)

証明可能安全性 (provable security) は暗号理論研究コミュニティの中ではこれまで２０年に渡って議論されてきたが、近年、この手法が新しい暗号技術標準を制定する上で重要な役割を果たしている。これにより、暗号研究者だけでなく現場の人間にまで、証明可能安全性により得られた安全性評価は実際にはどういう意味を持つのかという関心を起こさせている。また、証

明可能安全性の証明が public discussion を通して検証されるには時間がかかるという事実は幾分見逃されてきた感がある。この講演では、OAEP と ESIGN の２つのケーススタディをもとに、証明可能安全性理論がいかに微妙で難解な問題かが紹介された。Jacques Stern が示した"Provable security in five steps" は以下の通り。

1. Define goal of adversary
2. Define security model
3. Provide a proof by reduction
4. Check proof
5. Interpret proof

2.12. Cryptanalysis III (chair: *Josef Pieprzyk*)

On the Security of RDSA (*Pierre-Alain Fouque, Guillaume Poupard*)

RDSA は Biehl らにより提案された Schnorr 署名の variant である。本論文では RDSA が単純な既知文書攻撃(known-message attack)で攻撃可能であることを示した。具体的には、非常に少ない計算量で、既知のメッセージに対する 10 個未満の署名から署名鍵を導けることを示した。また、RDSA の修正版と、同じく Schnorr 署名の別の variant である GPS を比較し、GPS がほとんどのアプリケーションにおいて優位であることを示している。なお、GPS は NESSIE Portfolio に採用されている。

Cryptanalysis of the Public-Key Encryption Based on Braid Groups (*Eonkyung Lee, Je Hong Park*)

CRYPTO2000 で braid 群に基づく公開鍵暗号 BPKE が提案された。本論文では Burau 表現という braid 群の効率のよい表現を利用して BPKE の基盤となっている問題を解く手法を示した。この手法により、いくつかのパラメータについて、無視できない確率で、現実的な時間で公開鍵から秘密鍵を導けることが示された。この攻撃は ASIACRYPT2001 で示された BPKE の改良版にも適用できる。また、この攻撃に対して耐性をもつためのパラメータに関する要求条件も示された。

A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications (*Mihir Bellare, Tadayoshi Kohno*)

本論文では、ブロック暗号の安全性を議論する上で重要な、関連鍵攻撃 (related-key attack, RKA) に対する安全性を論じるための理論的手法を提案している。まず、RKA に対して安全な擬似ランダム置換と擬似ランダム関数の概念を定義し、どんなブロック暗号もこのような攻撃に対して安全性を示せないという否定的な結果と、RKA のあるクラスに対しては安全性が証明できるという肯定的な結果を示した。また、tweakable ブロック暗号など、関連鍵を使った様々なブロック暗号の構成法の安全性を示した。

2.13. Key Exchange (chair: *Matt Robshaw*)

Provably Secure Threshold Password-Authenticated Key Exchange (*Mario Di Raimondo, Rosario Gennaro*)

本論文で示された Password-Authenticated Key Exchange (PAKE) は、standard model (安全性の証明に random oracle を用いない) で安全性を証明できる初めての方式である。このモデルでは、パスワードは１つの認証サーバに保持されているのではなく、n ($> 3t$)台のサーバで共有されており、adversary は t+1 台のサーバを攻撃しないとパスワードが漏れないようになっている。この方式はサーバ・クライアント間のやりとりを最小にするために、コストのかかるゼロ知識証明を排除しており、実装も容易である。

A Framework for Password-Based Authenticated Key Exchange (*Rosario Gennaro and Yehuda Lindell*)

本論文では common reference string model における Password-Authenticated Key Exchange (PAKE)の一般化フレームワークが示された。著者らのプロトコルは Katz らの鍵交換プロトコルの抽象化であり、Cramer と Shoup により導入された smooth projective hashing の概念に基づいている。このフレームワークは、３つの抽象度の高い暗号ツールで記述されたモジュールプロトコルであり、安全性証明がモジュール単位でシンプルになったため、直感的に理解しやすくなったことが利点の一つである。

2.14. Information Theoretic Cryptography (chair: *Jean-Jacques Quisquater*)

The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations (*Ueli Maurer, Krzysztof Pietrzak*)

PRF (Pseudo-Random Function)を r 段の Feistel 構造に組み込んで PRP (Pseudo-Random Permutation)を構成する Luby-Rackoff 法について, 段数 r が大きい時の漸近

的なセキュリティを論じている．計算量的に無制限な adversary が URP (Uniform random permutation)と PRP を判別するために必要な query 回数を高々$O(2^{cn})$とした時に，$c < \alpha$ なる上界を考えると，段数 r と α は $\alpha = 1\text{-}O(1/r)$の関係にあることが示され，段数 r の増加とともに自明な上界である$\alpha = 1$ に近づくことが示されている．

New Bounds in Secret-Key Agreement: The Gap between Formation and Secrecy Extraction (*Renato Renner, Stefan Wolf*)

Alice と Bob と Eve がそれぞれ初期情報として X, Y, Z を持っている状態からスタートし，すべてのメッセージが Eve に盗聴されている状況下で，Alice と Bob が何ビットの鍵を Eve に知られずに共有できるか(Secret Key Rate)を考える．Maurer93 はこのレートが X, Y, Z によって決まる Intrinsic Information という量で上界が与えられるとしたが，著者らは Reduced Intrinsic Information という量で，よりタイトな上界が与えられるとしている．この差は Alice と Bob がプロトコルを通じて共通鍵を生成する能力の限界に起因している．

2.15. Secure Multi-Party Computation II (chair: *Yvo Desmedt*)

Round Efficiency of Multi-Party Computation with a Dishonest Majority (*Jonathan Katz, Rafail Ostrovsky, Adam Smith*)

Plain モデルの下で，static かつ passive な t 人 ($< n$) の不正利用者に対して定数ラウンドのマルチパーティ計算が構成できることが示されている．著者らの構成は Coin flipping により CRS (Common Reference String) を生成するフェーズと，Canetti らの STOC'02 の結果を用いて CRS モデルの下でマルチパーティ計算を実行するフェーズに分かれ，不正利用者を static かつ passive に限定することで coin-flipping とマルチパーティ計算を定数ラウンドで実現している．

Efficient Multi-Party Computation over Rings (*Ronald Cramer, Serge Fehr, Yuval Ishai, Eyal Kushilevitz*)

環上でのマルチパーティ計算の構成法について論じている．環を使う理由は，より一般的な数学的構造を扱え，効率が良くなるためだと主張している．定数ラウンドのマルチパーティ計算として Ishai-Kushilevit の Randomized Polynomials や Branching Program の環版を構成し，例として max 関数の計算を効率よく実行できることが示されている．

2.16. Group Signatures (chair: *Henry Gilbert*)

Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions (*Mihir Bellare, Daniele Micciancio, Bogdan Warinschi*)

グループ署名について従来考えられていた様々な要件は，Full Anonymity と Full Traceability の 2 つに帰着されることを示し，trapdoor permutation だけを仮定すれば 2 つの要件を満たすグループ署名が構成できることが示されている．

Extracting Group Signatures from Traitor Tracing Schemes (*Aggelos Kiayias, Moti Yung*)

グループ署名と Public Key Traitor Tracing の間の双対性を指摘し，Public Key Traitor Tracing からグループ署名に変換できると主張している．Boneh-Franklin を変換元にすれば署名サイズがグループメンバ数に依存しない（結託閾値に依存する）グループ署名が構成できることが示されている．

2.17. Rump Session (chair: *Stanislaw Jarecki*)

*** Cryptanalysis and Other Daring Attacks**

Cryptanalysis of Augot and Finiasz Cryptosystem of Eurocrypt 2003 (*Jean-Sebastien Coron, Gemplus, France*)

Cryptanalysis of the General Approach of the Polynomial-Reconstruction Based Public Key System (*Moti Yung, Columbia University, joint work with Aggelas Kiayias*)

Cryptanalysis of the Alleged SecureID Hash Function (*Alex Biryukov, KU Leuven, Belgium, joint work with Joseph Lano, Bart Preneel*)

On the Lenstra-Verheul Guidelines for Selecting Key Sizes (*Alain P. Hiltgen, UBS, Switzerland*)

A Linear Distinguishing Attack on Scream (*Alexander Maximov, joint work with Thomas Johansson, Lund Univ, Sweden*)

Cryptanalysis of the Solitaire cipher (*Marina Pudovkina, MPEI, Russia*)

(1) Chemical Combinatorial Attacks; and (2) PKZIP RSA (*David Naccache, Gemplus, France*)

*** Public-Key Crypto**

Lower Bounds on the Efficiency of Encryption and Digital Signatures (*Rosario Gennaro, IBM, USA, joint work with Yael Gertner, Jonathan Katz*)

How to Fool an Unbounded Adversary with a Short Key Even Better (*Adam Smith, USA, joint work with Yevgeniy Dodis*)

Public Key with Single Key per User with Escrow-Encryption and Non-Escrow Signing (*Moti Yung, Columbia University, USA, joint work with Homin K. Lee*)

Sequential Aggregate Signatures form Trapdoor Homomorphic Permutations (*Hovav Shacham, Stanford, USA*)

Parallel Signcryption from any trapdoor permutation (*Yevgeniy Dodis, USA, joint work with Michael Freedman, Shabsi Walfish*)

Subgroup Signatures and Constant Size Ring Signatures (*Yevgeniy Dodis, USA, joint work with Aggelos Kiayias, Antonio Nicolosi, Victor Shoup*)

*** Announcements about Standards, Standard Groups, Conferences, and Plagues**

New European Schemes for Signatures, Integrity, and Encryption (*Bart Preneel, KU Leuven, Belgium*)

2nd International Security in Storage Workshop (*James Hughs*)

IEEE Security in Storage Standard Group (*James Hughs*)

RusCrypto (*Anatoly Lebedev, LANCrypto, Moscow*)

ASIACRYPT 2003 (*Chi-Sung Laih, Taiwan*)

*** Exotic, Quantum, and Multi-Party Stuff**

Secure Multiplication of Shared Secrets in the Exponent (*Rosario Gennaro, IBM, USA, joint work with Mario Di Raimondo, U. of Catania, Italy*)

Graphs in cryptography, protocol for new optics (*Kamil Kulesza, Polish Academiy of Science, joint work with Zbigniew Kotulski*)

Geometry of Compact Manifolds in Cryptography (*Laszlo Csimras, Hungary*)

On the Power of Quantum Memory (*Renato Renner, joint work with Robert Konig, Ueli Maurer*)

Cryptography, CS, and Quantum Computing Research Program Testing (*Steve Meyer, USA*)

Honey, I shrunk the Bank Notes (*Marc Joye, France, joint work with David Naccache*)

*** Ciphers**

Twirl Twiddles Too (*Arjen Lenstra, joint work with Hughs, Leyland, Dodson*)

On the Additive Differential Probability of Exclusive-Or (*Johan Wallen, Finland, joint work with Philippe Dumas, Helger Lipmaa*)

The unicity distance of GI stream ciphers (*Marina Pudovkina, MPEI, Russia*)

Rabbit: A New High-Performance Stream Cipher (*Ove Scavenius, Cryptico, Denmark, joint work with Martin Boesgaad, Mette Vesterager, Thomas Pedersen, Jesper Christiansen*)

On Designing Fast Ciphers Based on Data-Dependent Operations (*Nick A. Moldovyan*)

Now that FAGCI is dismissed, what follows? (*Anatoly Lebedev, LANCrypto, Russia*)