パネルディスカッション
公開鍵暗号技術の最新動向について

北陸先端科学技術大学院大学

情報科学研究科

宮地　充子

目次

楕円曲線暗号の紹介
公開鍵暗号の RSA と楕円曲線暗号の比較
ISOにおける公開鍵暗号技術の標準化動向

1. 楕円曲線暗号
2. 楕円曲線暗号とRSA暗号の違い
3. ISO規格の原理，枠組み，規格の構成
4. ISO規格制定までの過程
5. 主な公開鍵暗号のISO規格

MiYaJi Laboratory

自己紹介

JAIST 20th ANNIVERSARY JAIST JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990

- 所属：北陸先端科学技術大学院大学・附属図書館長
  - ディジタルライブラリの一環で，貴重図書のディジタル化やリポジトリ登録（論文のディジタル配布）．著作権保護などのセキュリティ技術が必須．
- 情報セキュリティ技術の国際標準化活動
  - 2000年よりeditor として国際規格の作成
  - 15946-4, 9796-3, 15946-1, 18014, 15946-5 の国際規格作成
  - 18033－4の国際規格の作成中
- 情報セキュリティ国際学会への貢献
  - 52 International Conf のPC委員/委員長
  - 2 International Journal のeditor
- 情報セキュリティに関する研究及び教育
  - 数学的観点での情報セキュリティの研究
    - 楕円曲線暗号（加算連鎖，楕円曲線の構成）

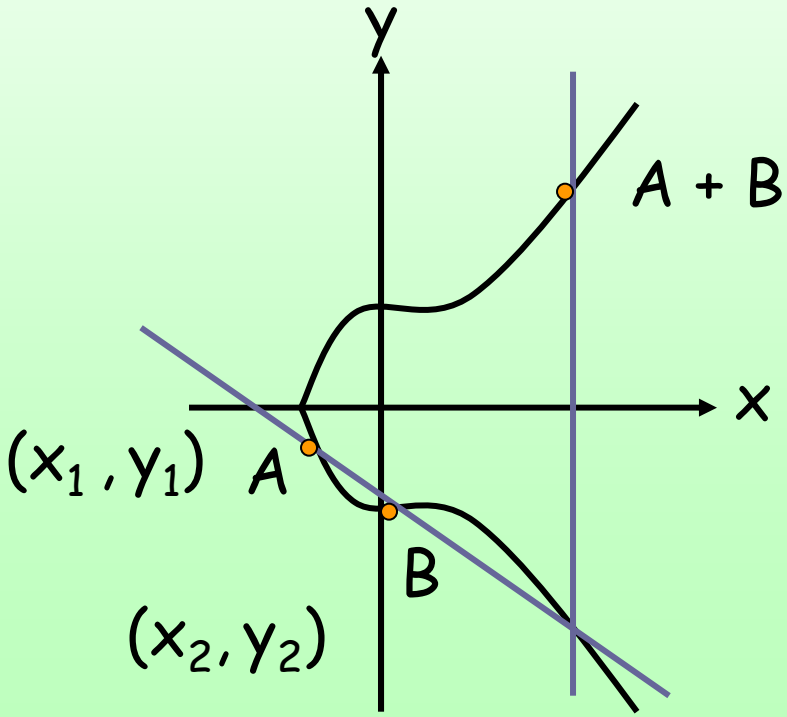
楕円曲線(Elliptic Curve)

A non-degenerate cubic curve

$E: y^2 = x^3 + ax + b$ $(a, b \in F_p (p>3),\ 4a^3+27b^2 \neq 0)$

Feature

- Addition is defined.→ E is a group.
- Addition is computed easily.



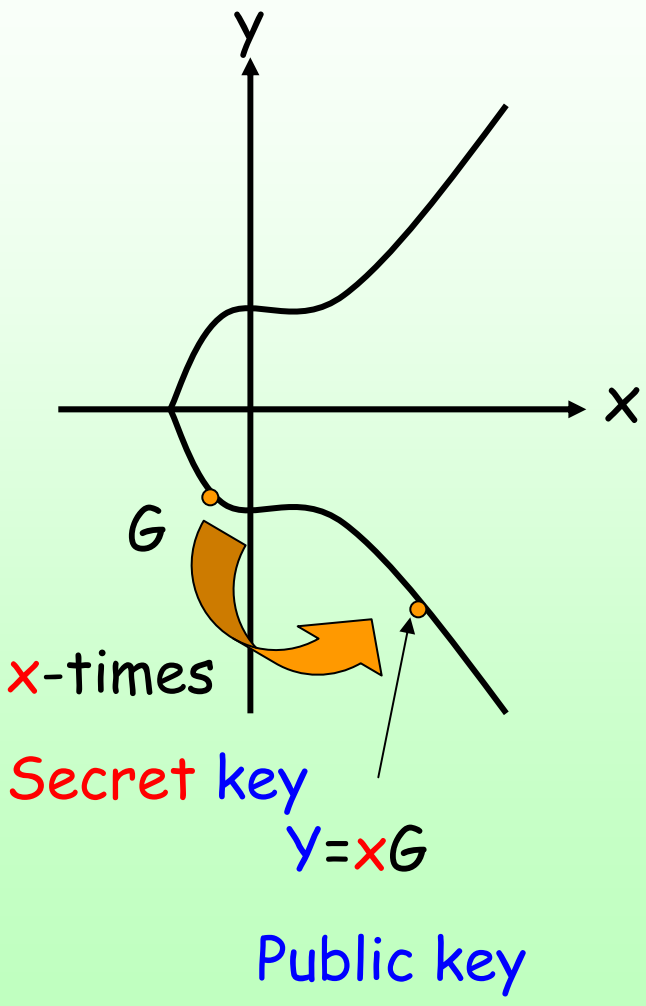
$A + B = (x_3, y_3)$ $(A \neq B)$

$x_3 = ((y_2-y_1)/(x_2-x_1))^2 - x_1-x_2$

$y_3 = (y_2-y_1)(x_2-x_1)(x_1-x_3)-y_1$

computed by a few multiplications.

楕円曲線上の離散対数問題 (ECDLP)



ECDLP is defined over

$E(F_p)$
$=\{(x,y) \in F_p \times F_p \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$
$E(F_p)$ is a finite abelian group.

ECDLP

For given G, $Y \in E(F_p)$, find x such that $Y = G + \cdots + G = xG$

ECDLP VS DLP/IF

Security

- Any DLP/IF is solved faster than an exhaustive algorithm.
- Well-chosen ECDLP is solved only in an exhaustive algorithm.

→ECDLP is more efficient than DLP/IF with the same security level.

- Key size of ECDLP vs DLP/IF: 1/6 (before) → 1/9 (2010)

Other Good Features

- Abundant resources of cryptosystems (暗号資源の豊富性)

One DLP/IF is available for one definition field (architecture).
Many ECDLP is available for one definition field (architecture).
→This is very useful to update a cryptosystem.

- There exist useful bilinear pairings (双線形写像) on an elliptic curve. define the new security base BDHP

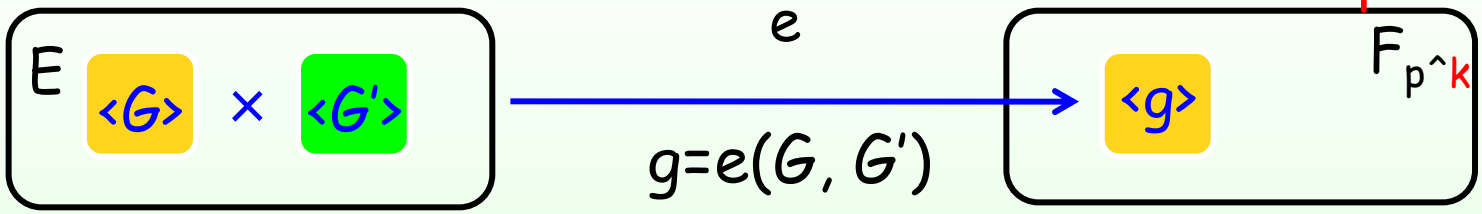
→resolve some open problems in the cryptology.

双線形写像を用いる暗号

A bilinear pairing

Elliptic curve: addition

Finite Field: multiplication



Features

Bilinear: $e(aG, bG') = e(G, G')^{ab}$
keep additions on E to mult on F_p.

Non-degenerate: $g=e(G, G') \neq 1$
A subgroup in E, <G>, is isomorphic to a subgroup in F_{p^k}, <g>.

- Connect ECDLP and DLP.
- Both features are available.

Bilinear Diffie-Hellman Problem (BDHP)

For given aG, bG, aG', cG' in E, compute $e(G, G')^{abc}$ in F_{p^k}

→ Some open problems in the cryptology have been solved.

ISO/IEC JTC1/SC27

国際標準化機構/国際電気標準会議で設置した情報セキュリティ技術全般の国際標準を決定する委員会.

- WG1:情報システムにおけるセキュリティ要求条件，セキュリティサービス，セキュリティガイドライン.
- WG2:情報セキュリティ技術のアルゴリズム及びプロトコル
- WG3:セキュリティ評価及びその評価手法に関わる要求事項，暗号モジュールの耐タンパー性など.
- WG4:侵入検知，ネットワークセキュリティサービス，ビジネス継続プラン
- WG5:バイオメトリクス技術，プライバシー，ID管理(独 議長)
- SC27は毎年春と秋に国際標準化会議.

('06/5に体制変更)

SC27/WG2の主な審議規格

- 15946 楕円曲線に基づく暗号技術
- 18031 乱数生成

→ 暗号基盤関連

- 9796 メッセージ復元型ディジタル署名
- 14888 添付型ディジタル署名
- 10118 ハッシュ関数
- 18033 暗号アルゴリズム
- 29192 軽量暗号

→ 暗号理論関連

- 29150 署名付き暗号
- 19772 認証付き暗号化
- 11770 かぎ管理
- 9797 メッセージ認証コード
- 9798 エンティティ認証
- 10116 n ビットブロック暗号の利用モード
- 13888 否認防止
- 18014 タイムスタンプサービス

→ 暗号応用関連

- 検討期間（WG2 ロードマップ，暗号アルゴリズムと鍵長）

国際標準に関する全過程

- 国際標準に関する全過程:

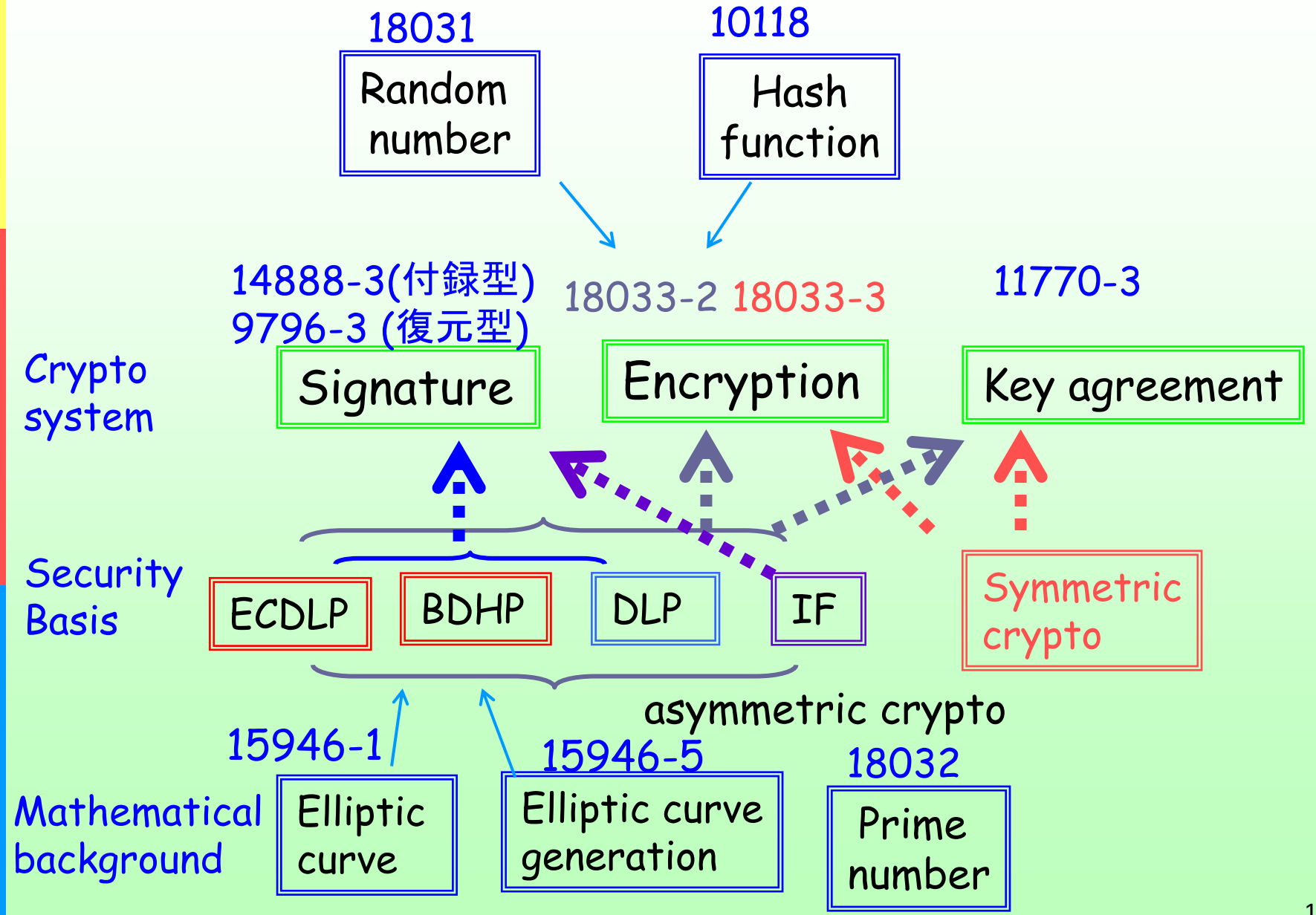
Study Period → NP→ WD→CD→ FCD→FDIS→IS ─ AMD / COR / 定期見直し

標準化検討期間　　国際規格作成段階　　国際規格発行後

Editor (編集者)
WD から FDIS までの期間の原案の作成，各国の意見の取りまとめ.
WD → CD への移行は各国投票で決定 (3 ヶ月の投票期間)
CD → FCDへの移行は各国投票で決定 (4ヶ月の投票期間)
FCD → FDISへの移行は各国投票で決定 (2ヶ月の投票期間)

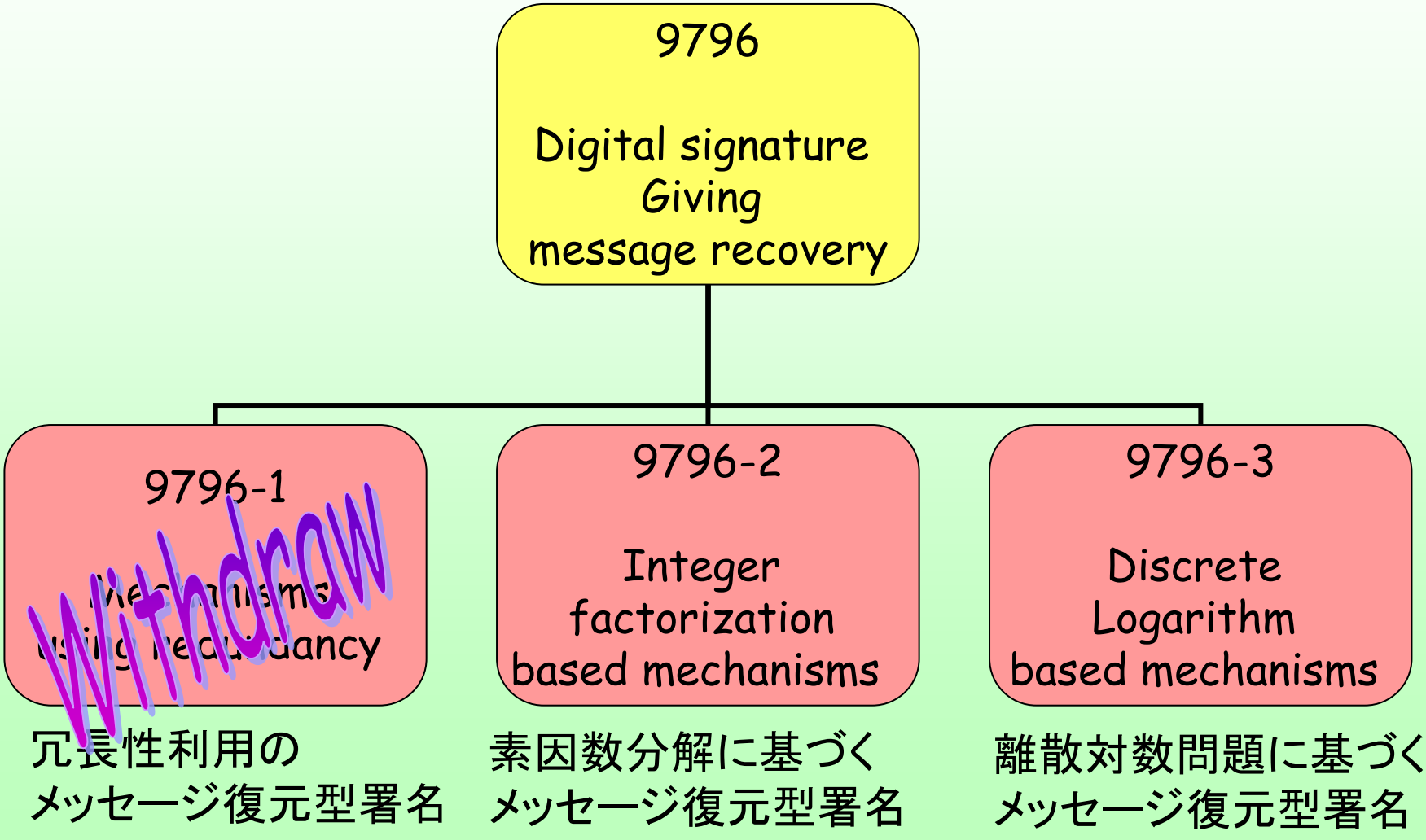
IS 後，約3年後に定期見直し

情報セキュリティのISO規格



ISO規格の枠組み (例 ディジタル署名)

機能毎に規格化



楕円曲線暗号の ISO標準化動向

15946
楕円曲線暗号

15946-1
総論

第二版
発行07
(宮地)

15946-2
付録型署名

Withdraw

15946-3
鍵共有

Withdraw

15946-4
復元型署名

Withdraw

(宮地)

15946-5
楕円生成

(宮地)
第一版発行09

9796
復元型署名

9796-2
素因数分解

9796-3
DLP

(宮地)

第二版発行07

14888
付録型署名

14888-2
素因数分解

14888-3
DLP

第二版発行07

11770
鍵共有

11770-1
総論

11770-2
共通鍵

11770-3
公開鍵

第二版
発行08

メッセージ復元型ディジタル署名9796

- 第2部　素因数分解に基づく規格
  - ’05/5定期見直し
    →ISO/IEC9796-2:2002010-01(2nd edition)継続使用
  - ’08/4 定期見直しで改訂決定.
    - 追補（08年発行）の統合が主な改訂理由
  - ハッシュ関数利用のRSA署名

- 第3部 離散対数問題に基づく規格
  編集者：宮地 (JAIST) ’06 年に国際規格発行
  - NR, ECNR(フィンランド), ECMR,ECAO(日本), ECKNR（韓国), ECPV(US) 掲載
  - 2009年に定期見直し→継続使用

添付型デジタル署名14888

- 第1部 総論:
  - 編集者:大塚　玲(日本), 08年に国際規格発行
- 第2部 因数分解に基づく機構:
  - 編集者:Louis Guillou(仏), 08年に国際規格発行
  - RW (Rabin-Williams), RSA-PSS(米), GQ1, GQ2, GPS1, GPS2(仏), ESIGN (日)
- 第3部 離散対数に基づく機構:
  - 編集者:Liqun Chen(英)- Pil John Lee(韓), 06年に国際規格発行
  - 証明書方式:DSA(US), EC-DSA(カナダ), EC-GDSA(独), KCDSA, EC-KCDSA(韓), IDベース方式: Hess02(英), Cha-Cheon02(韓)
  - Rossian ECDSA の追補

    ロシア国内利用されている方式の規格提案.

    Schnorr 署名の特許が有効期限を迎えたので追加を決定.

楕円曲線暗号技術15946

- 楕円曲線暗号関連の国際規格
- 第1部 楕円曲線全体の規格:
  - 編集者:宮地，08年に国際規格発行
  - 2002年版の国際規格の改訂(2005年4月開始決定).
  - 楕円曲線暗号を実現に必要な技術の規格．楕円曲線の諸性質，楕円曲線の加算公式，べき演算，双線形写像など.
- 第2-4部は第1版の国際規格を廃止
  - 11770-3, 14888-3, 9796-3が発行されたことによる.
- 第5部 楕円曲線生成
  - 編集者:宮地，09年に国際規格発行
  - 楕円曲線暗号，双線形暗号の楕円曲線生成に関する規格.
  - ランダム曲線，CM曲線などをサポート.

かぎ管理(11770)

- 第3部:非対称暗号技術を用いる鍵確立機構
  - 1999年版の改訂(編集者:S.Savard(カナダ)).
  - 対称暗号に使用する秘密鍵の共有/配送方式, 公開鍵の配送方式.
  - 楕円曲線を利用した鍵確立機構15946-3 統合.
  - その他双線型写像を利用したアルゴリズムがない.
  - 2008年. 第二版IS出版.

まとめ

- 楕円曲線暗号 VS 素因数分解問題ベースの暗号
  - 既存攻撃の観点からの鍵サイズの利点
  - 数学的観点での研究資源の違い
- ISO/IEC JTC1/SC27/WG2
  - 情報セキュリティのアルゴリズム及びプロトコルに関する国際標準化規格の策定を進める
  - 最新研究動向・特許動向と密接に連動
  - 双線形写像に基づく暗号の標準化は今後