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

モデレータ: 高木　剛（公立はこだて未来大学）
パネリスト:　田中圭介（東京工業大学）
宮地充子（北陸先端科学技術大学院大学）
伊豆哲也（富士通研究所）

各パネラーの話題

- 田中圭介 (東工大)
  公開鍵暗号の安全性証明技術
  新しい公開鍵暗号

- 宮地充子 (JAIST)
  楕円曲線暗号について
  ISOにおける公開鍵暗号技術の標準化動向

- 伊豆哲也 (富士通)
  公開鍵暗号の解読実験
  公開鍵暗号の鍵長の選択

- 高木剛 (はこだて未来大学)
  2009年度CRYPTRECリストガイドWGより、IDベース暗号

2009年度リストガイドWG

主　査：　高木　剛　　(公立はこだて未来大学)

委　員：　金岡　晃　　(筑波大学大学院)
　　小林　鉄太郎　(日本電信電話株式会社)
　　白石　善明　　(名古屋工業大学)
　　高島　克幸　　(三菱電機株式会社)
　　田中　秀磨　　(情報通信研究機構)
　　花岡　悟一郎　(産業技術総合研究所)

執筆協力者：　市川　幸宏　(三菱電機株式会社)
　　草川　恵太　(東京工業大学)

IDベース暗号

- 公開鍵の例

RSA暗号 → 2個の素数の積

n = 826ed558a0f0cba7ae09485abf80c544837efeb7116153f5d6479d5945fdb6c61f50c984445d601d85eceb6b
ad9f700b90ae28984dd590f5ca3e6ed968a3ca32a5cf584992d92590ae9ed4f81b70d008a9e4a16905925dbb
79d82b67dc6b70869a83f037c147d298c0e2eea5f858f3881ad1071c5c221ecb795d78b68bae7863

楕円曲線暗号 → 楕円曲線上のランダムな点

x = 4a96b568 8ef57328 46646989 68c38bb9 13cbfc82
y = 23a62855 3168947d 59dcc912 04235137 7ac5fb32

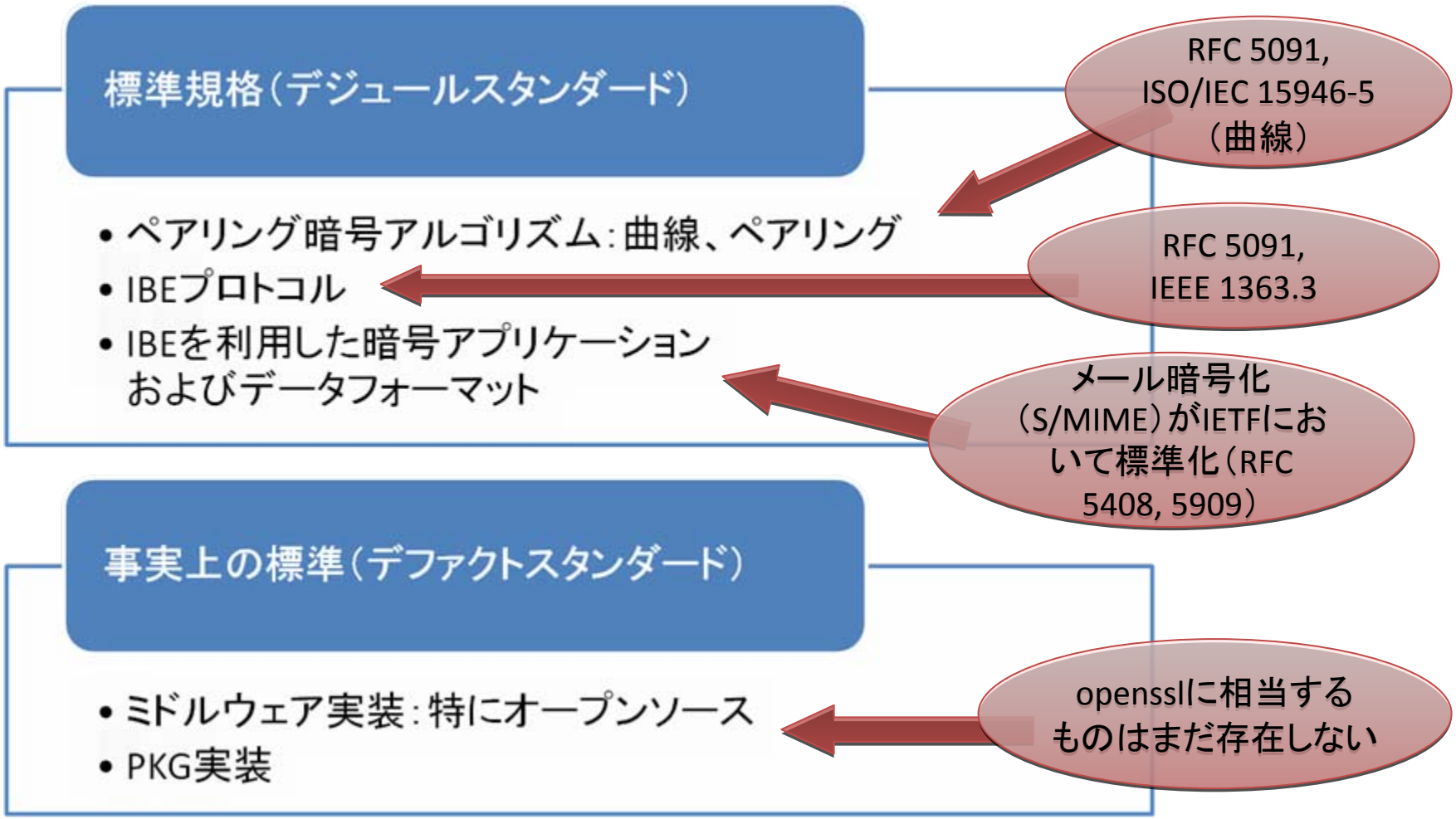
IDベース暗号 → 鍵長以下の自由なビット列
(氏名、email アドレス，携帯電話の番号，基礎年金番号など)

現在のPKIとIDベース暗号の比較

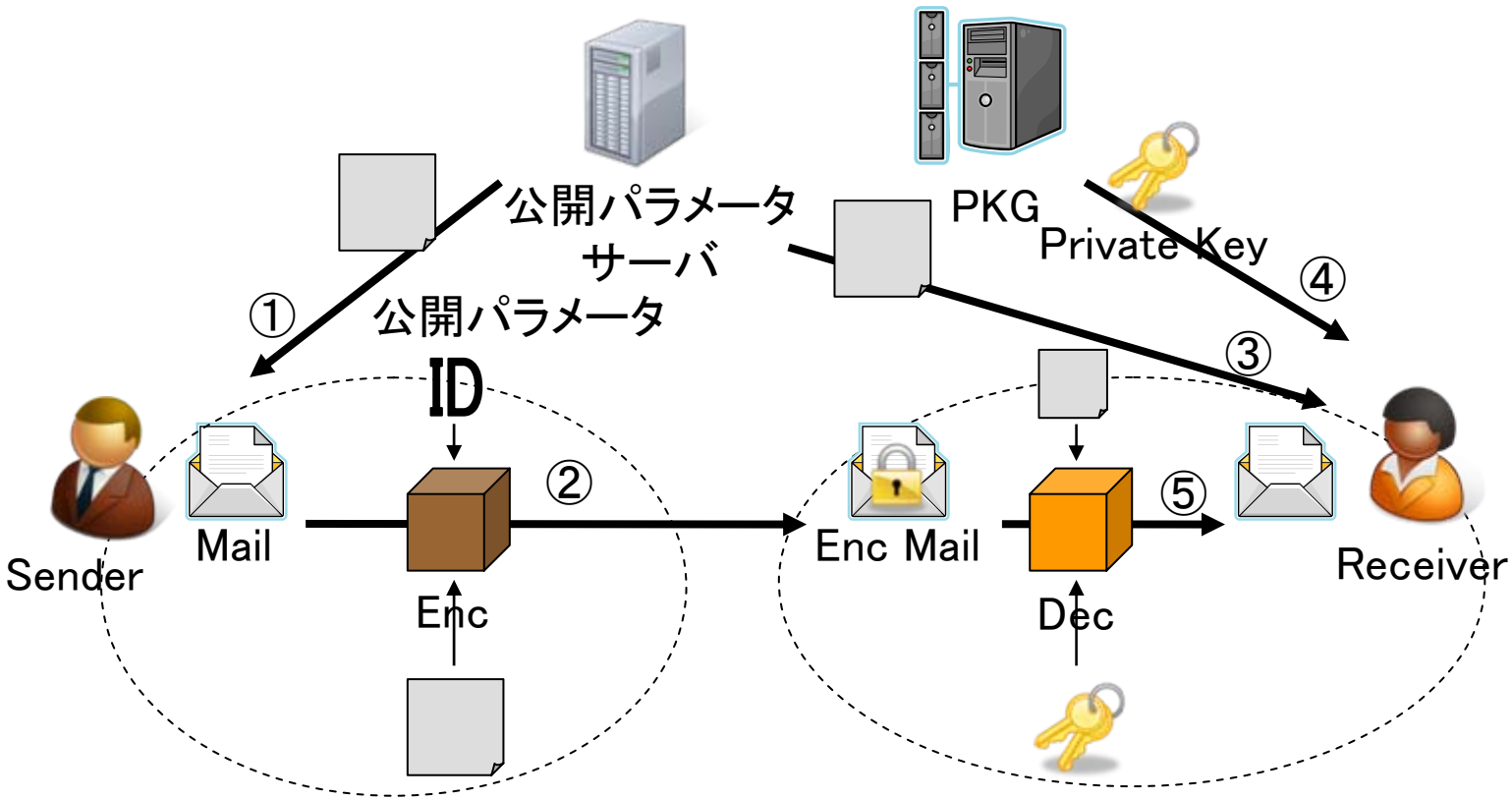
	現在のPKI	IDベース暗号
ID情報と公開鍵のバインディング	必要	不要
CAやPKGの信頼性 （公開鍵や公開パラメータの信頼性）	必要	必要
秘密鍵データの生成者	利用者/PKI事業者	鍵生成センタ（PKG） （利用者は生成できない）
秘密鍵データの生成時期	サービス利用前	サービス利用前後問わず

IDベース暗号の社会基盤化に向けた3つの視点

IDベース暗号の必要な標準化



IDベース暗号メールシステム



参考情報

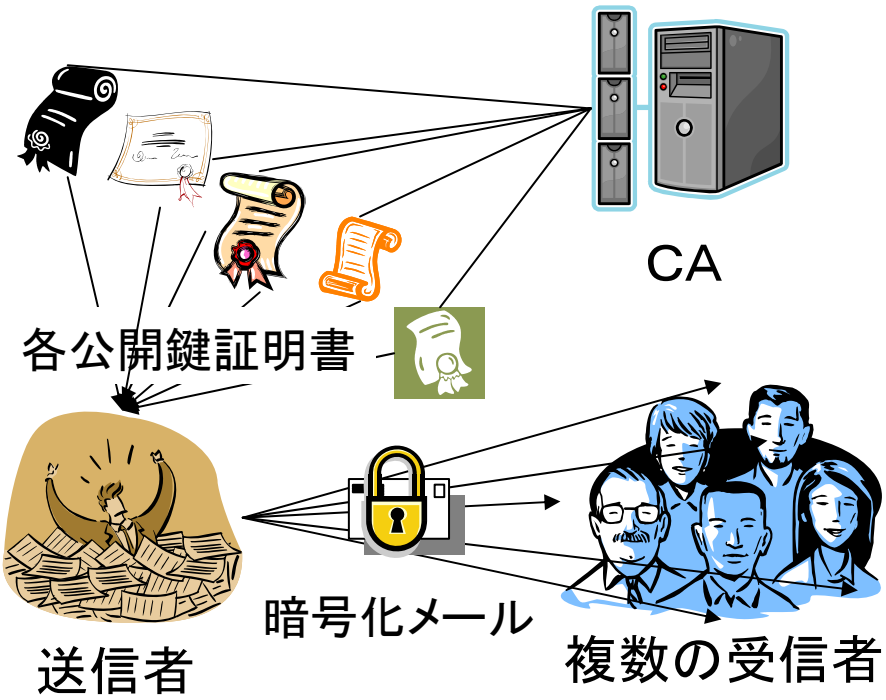
RFC5408: Identity-Based Encryption Architecture and Supporting Data Structures.

RFC5409: Using the Boneh-Franklin and Boneh-Boyen Identity-Based Encryption Algorithms with the Cryptographic Message Syntax (CMS).

公開鍵証明書を必要としないIDベース暗号が注目

暗号化メールに適用した場合

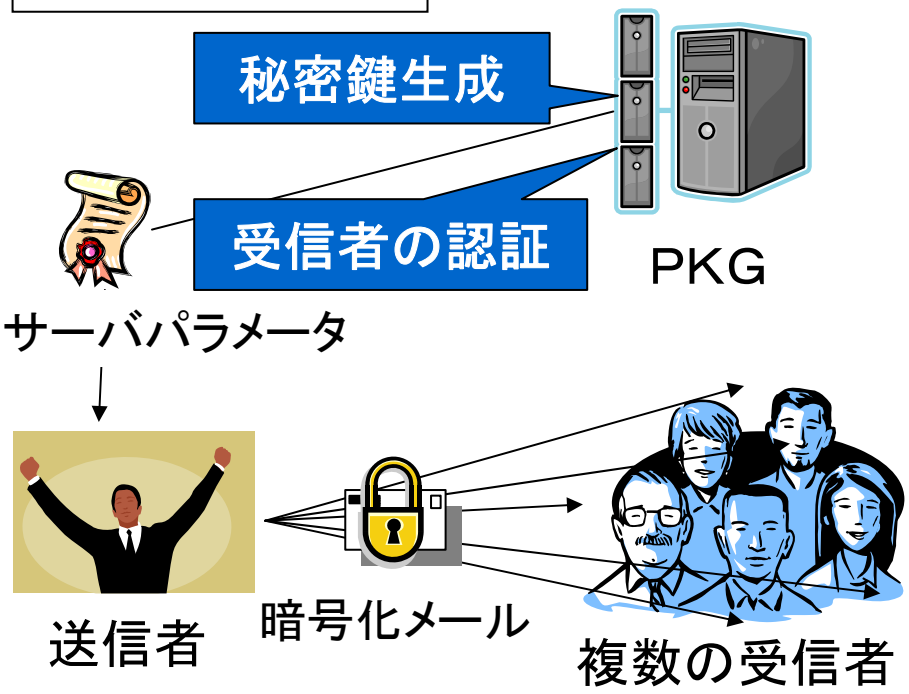
PKI



事前に複数の公開鍵証明書必須

受信者ごとに公開鍵証明書を管理

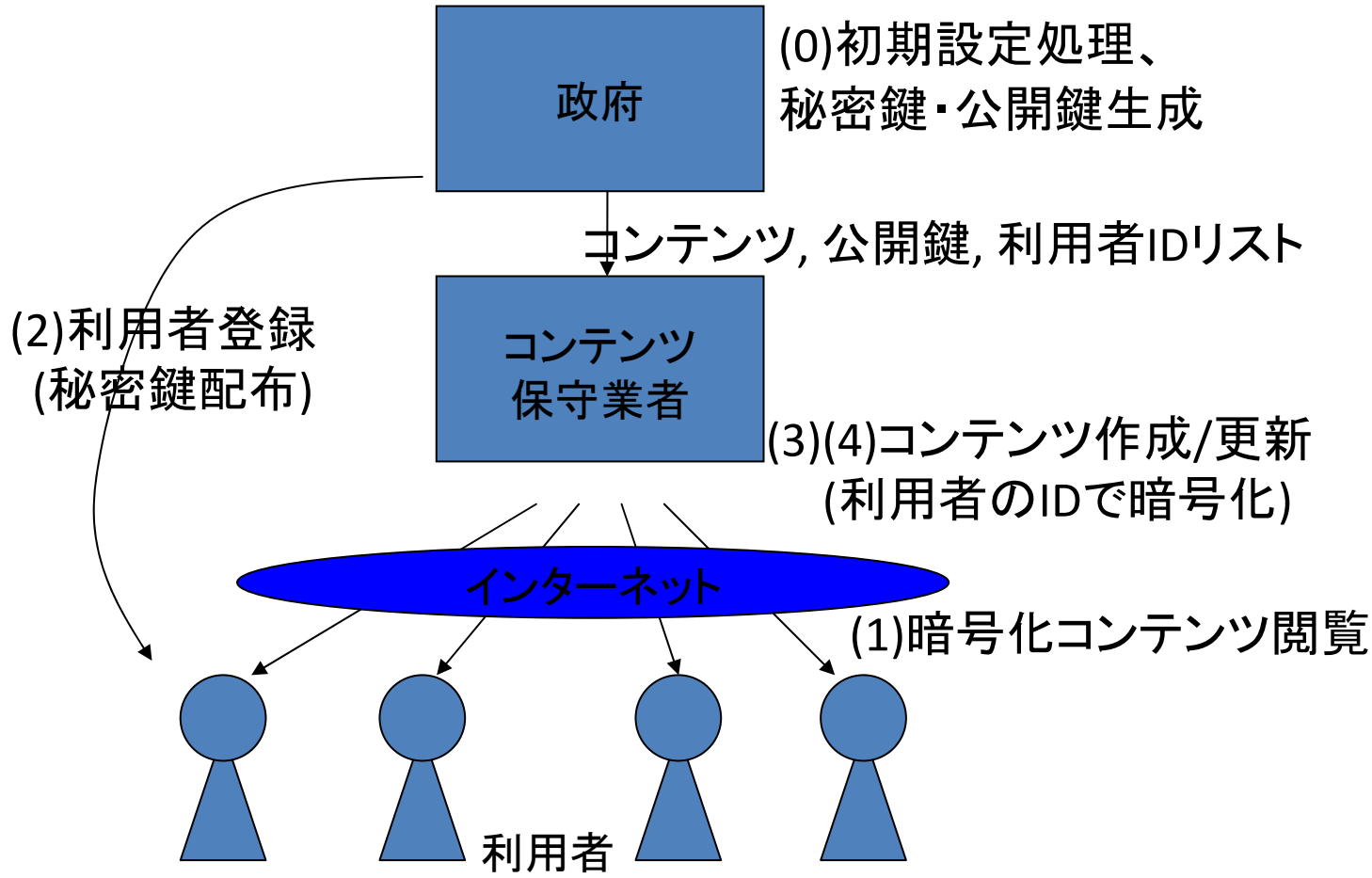
IDベース暗号



事前に単数のパラメータ必須

公開鍵＝IDであるため特殊な管理不要

Webシステム全体図



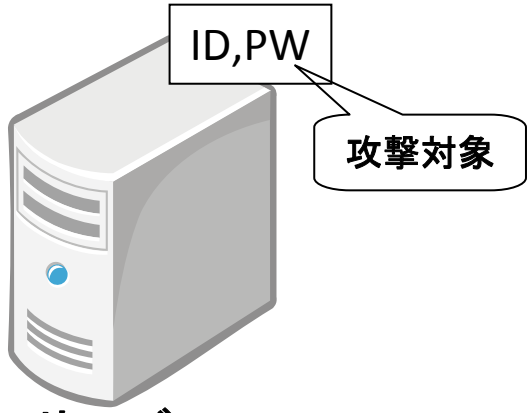
参考情報:「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」
2007 年**11** 月 内閣官房情報セキュリティセンター

パスワードPW利用

利用者端末

1.IDとPWを送信

2. ID,PWを
確認



Webサーバー

3.コンテンツを送信

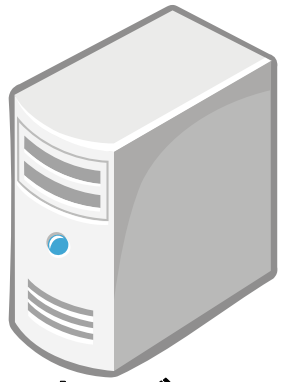
IDベース暗号利用

利用者端末

1.IDを送信

2.暗号化された
コンテンツを送信

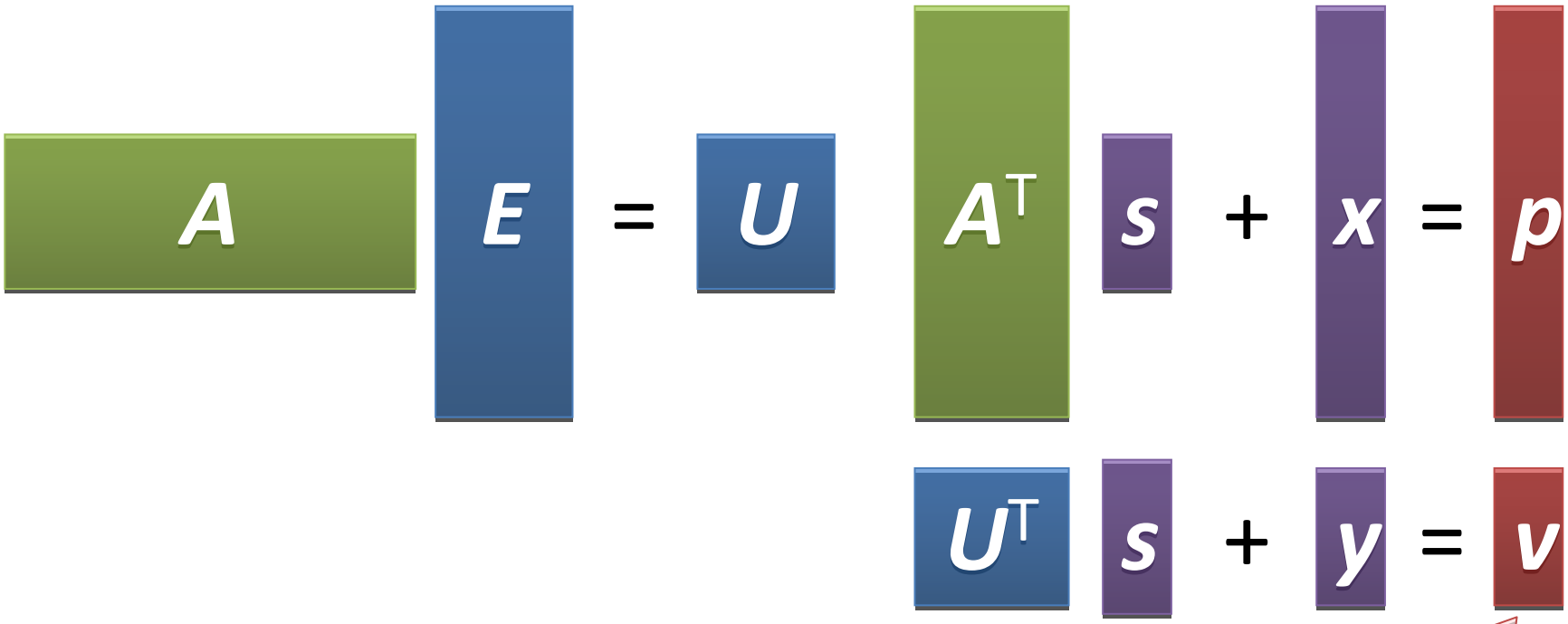
3. ID,SIDを用いて
暗号化された
コンテンツを復号



Webサーバー

格子問題に基づく暗号

- IDベース暗号
  - Gentry, Peikert, Vaikuntanathan: Trapdoors for hard lattices and new cryptographic constructions. STOC 2008.
  - Agrawal, Boyen: Identity-Based Encryption from Lattices in the Standard Model unpublished manuscript, 2009.
  - Peikert: Bonsai Trees (or, Arboriculture in Lattice-Based Cryptography), Cryptology ePrint Archive: Report 2009/359.
  - Cash, Hofheinz, Kiltz: How to Delegate a Lattice Basis, Cryptology ePrint Archive: Report 2009/351.
  - Boneh, Boyen: Efficient Lattice (H)IBE in the Standard Model from the BB-1 Framework, rump session talk at CRYPTO 2009.
  - Stehlé, Steinfeld, Tanaka, Xagawa: Efficient Public Key Encryption Based on Ideal Lattices. ASIACRYPT 2009.
- CCA安全な公開鍵暗号
  - Peikert, Waters: Lossy Trapdoor Functions and their Applications. STOC 2008, 187-196.
- 完全準同型暗号
  - Gentry: Fully Homomorphic Encryption Using Ideal Lattices. STOC 2009, 169-178.



Ext: Generate $\boldsymbol{E}$

Enc: $(\boldsymbol{p}, \boldsymbol{v} + \boldsymbol{w}\mathrm{q}/2)$

Dec: $\boldsymbol{d} = \boldsymbol{v} - \boldsymbol{E}^{\mathrm{T}}\boldsymbol{p} = \boldsymbol{w}\mathrm{q}/2 + \boldsymbol{y} - \boldsymbol{E}^{\mathrm{T}}\boldsymbol{x} \approx \mathbf{w}\mathrm{q}/2$

一様分布と
識別不可能

公開鍵暗号の解読実験

- 676ビット　有限体上の離散対数問題DLP

  2009年12月9日、(NICT、公立はこだて未来大学)

  http://www2.nict.go.jp/pub/whatsnew/press/h21/100223/100223.html

- 768ビット　素因数分解

  2009年12月12日、(NTT、ボン大学、EPFL、INRIA、CWI)

  http://www.ntt.co.jp/news2010/1001/100108a.html

報道資料

公立はこだて未来大学
FUTURE UNIVERSITY-HAKODATE

NiCT National Institute of Information and Communications Technology

平成22年2月23日
情報通信研究機構
公立はこだて未来大学

公開鍵暗号の安全性の根拠となる計算で世界記録を更新

～ 676ビット長の「有限体上の離散対数問題」を汎用コンピュータによって33日間で計算 ～

独立行政法人情報通信研究機構（以下「NICT」という。理事長：宮原 秀夫）は、公立はこだて未来大学（学長：中島 秀之）との共同研究として、「有限体上の離散対数問題」*1について、これまでの世界記録を大幅に上回る676ビット長（10進数で204桁に相当）の計算に挑戦し、解読に必要なコンピュータの能力評価に初めて成功しました。公開鍵暗号*2では、この問題の計算が困難であることが安全性の根拠となっています。今回の成果は、現在広く利用されている1024ビット長の暗号が直ちに安全でなくなったことを示すわけではないものの、より強い暗号技術を将来導入する必要があることを示唆する結果であることから、国際標準を決定するISOや、我が国の電子政府に採用すべき暗号を推奨するCRYPTRECプロジェクト*3などの場において、その導入時期を検討するための重要な技術的根拠となります。

有限体上のDLP計算世界記録

有限体	GF(p)	GF(2^n)	GF(p^3)	GF(p^{30})	**GF(3^{6n})**
著者	Kleinjung et al	Joux et al	Joux et al	Joux, Lercier	**本実験**
日付	2007/2/5	2005/9/22	2006/8/23	2005/9/11	**2009/12/09**
アルゴリズム	NFS	FFS	NFS	FFS	**FFS**
関係探索ステップ	Many CPUs	16 Itanium2 × 4ノード	16 alpha processor	16 alpha processor	**Xeon (2.83 GHz) 計96コア**
線形代数ステップ	12-24 Xeon (3.2GHz)	16 Itanium2 × 4ノード	16 alpha processor	16 alpha processor	**Xeon (2.83 GHz) 計80コア**
計算時間	33日	17日	19日	0.5日	**33日**
ビット長	532	613	394	556	**676**