パネル1
公募対象カテゴリを中心とした暗号技術の動向について

モデレータ　高木剛（はこだて未来大学)

パネリスト　大塚 玲（産業技術総合研究所)

下山 武司（富士通研究所)

盛合 志帆（ソニー)

吉田 博隆（日立製作所)

パネリスト担当

公募対象の暗号技術＋ハッシュ関数＋IDベース暗号

(1) ブロック暗号 ⇒ 盛合
(2) 暗号利用モード ⇒下山
(3) メッセージ認証コード ⇒ 下山
(4) エンティティ認証 ⇒ 大塚
(5) ハッシュ関数 ⇒ 吉田
(6) IDベース暗号 ⇒ 高木

2008年度IDベース暗号WG

主　査:

高木　剛　　はこだて未来大学

委　員:

伊豆　哲也　富士通研究所

岡本　健　　筑波技術大学

小林鉄太郎　NTT情報流通プラットフォーム研究所

境　隆一　　大阪電気通信大学

高島　克幸　三菱電機

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

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)

IDベース暗号の歴史

1984：岡本(龍), Shamir，IDベース暗号の概念

1985~: KPS，ID-NIKS, 合成数の離散対数問題など

2001: 境-大岸-笠原, Boneh-Franklin
ペアリングを利用した効率的な方式

2004: Boneh-Boyen1,2,3
2005: Waters 方式
2006: Gentry 方式

最近の動向

- IEEE P1363.3, http://grouper.ieee.org/groups/1363/IBC/index.html
- RFC5091 (December 2008): Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems
- NIST Workshop, Applications of Pairing Based Cryptography: Identity Based Encryption and Beyond, June 3-4, 2008.
- 「世界で少なくとも600万人が使用している」L. Martin, “Identity-Based Encryption Comes of Age”, IEEE Computer, pp. 93–95, August 2008.

ペアリングの実装データ（PC）

- AES-80セキュリティ　(160-bit ECC, 1024-bit RSA)
  - 0.53 ms (η Tペアリング、Core 2 Duo, 2並列)
  - 2.61 ms (η Tペアリング、Opteron 275)
  - 3.16 ms (Ateペアリング、Pentium 4)

- AES-128セキュリティ (256-bit ECC, 3072-bit RSA)
  - 16.4 ms (η Tペアリング、Pentium 4)
  - 16.3 ms (η Tペアリング、Opteron 275)
  - 10.5 ms (Ateペアリング、Pentium 4)

ペアリング暗号

- 鍵隔離暗号 (Key-Insulated Encryption)
- 代理再暗号化 (Proxy Re-encryption)
- キーワード検索暗号 (Keyword Searchable Encryption)
- 放送暗号 (Broadcast Encryption)
- グループ署名 (Group Signature)
- 属性暗号 (Attribute-based Encryption)
- ・・・

IDベース暗号の検討課題