世界の暗号標準化動向

NESSIEの活動について

2001年4月18日

三菱電機情報技術総合研究所

松井　充

NESSIE プロジェクトとは

- 欧州における暗号アルゴリズム評価プロジェクト
  New European Schemes for Signatures, Integrity, and Encryption
- 暗号専門家グループが主催
  Coordinator: Bart Preneel（ベルギー・レーベンカトリック大学）
- 2000年1月から2002年12月までの3年計画
- AESと同じく公募を行なったのち選考する
- “Industrial board” から企業の意見を聞く仕組み
- http://cryptonessie.org/

NESSIE プロジェクト計画

2000年1月	NESSIEプロジェクト開始
2000年3月	公募要項公開
2000年9月	公募締め切り
2000年11月	第1回 NESSIE 会議開催
2001年9月	第2回 NESSIE 会議開催
2002年2月	第1次選考
2002年10月	第3回 NESSIE 会議開催
2002年12月	最終選考

第1回 NESSIE 会議

- 2000年11月13,14日　ﾍﾞﾙｷﾞｰ・ﾚｰﾍﾞﾝｶﾄﾘｯｸ大学
- 応募暗号の応募者による発表
- 応募暗号総数約40本
- 日本からの投稿8本
- ブロック暗号の投稿が17本　あとは少なめ
- 暗号の紹介が主で安全性/実装性の比較はなし
- すでに2本が解読（理論的解読を含む）

NESSIE 応募暗号一覧

公開鍵（守秘）	ACE	IBM	共通鍵（ストリーム）	BMGL	Hastard 他	Leviathan	Cisco
	ECIES	Certicom		LILI-128	Dawson 他	SOBER-t16	Qualcomm
	EPOC	NTT		SNOW	Johansson他	SOBER-t32	Qualcomm
	PSEC	NTT	共通鍵（64ビットブロック）	CS-Cipher	CS Communication & Systems		
	RSA-OAEP	RSA		Khazad	Baretto, Rijmen		
公開鍵（認証）	GPS	France Telecom		MISTY1	三菱電機	Nimbus	Machado
公開鍵（署名）	ACE	IBM		Hierocrypt-L1	東芝	IDEA	Mediacrypt
	ECDSA	Certicom	共通鍵（128ビットブロック）	Anibus	Baretto, Rijmen		
	ESIGN	NTT		Caemellia	NTT, 三菱電機		
	FLASH	BULL CP8		Grand Cru	Borst		
	QUARTZ	BULL CP8		Noekeon	Daemen 他		
	SFLASH	BULL CP8		Q	McBride		
	RSA-PSS	RSA		SC2000	富士通		
メッセージ認証	Two-Track-MAC	Boer, Rompay	共通鍵(160ビット)	SHACAL	Gemplus		
	UMAC	Rogaway 他	共通鍵(複数ビット)	RC6	RSA	NUSH	LAN Crypto
ハッシュ関数	Whirlpool	Baretto,Rijmen		SAFER++	Cylink	5	

NESSIE プロジェクトの今後

- NESSIEの最終目標は産学の「コンセンサス」
  - ISO 等の標準化活動へのはたらきかけ
- 選考方法や選定アルゴリズム数は未定
  - 必ずしも1つに絞り込むことが目標ではない
- IPR (Intellectual Property Rights) Jungle
  - NESSIE は応募アルゴリズムの IPR に対する強制力をもたない
- 選考結果は大きな影響力をもつ可能性
  - 幅広い対象、超一流の主催者グループ、Industrial board との協調