PSEC-KEM暗号評価の現状報告（スクリーニング評価）

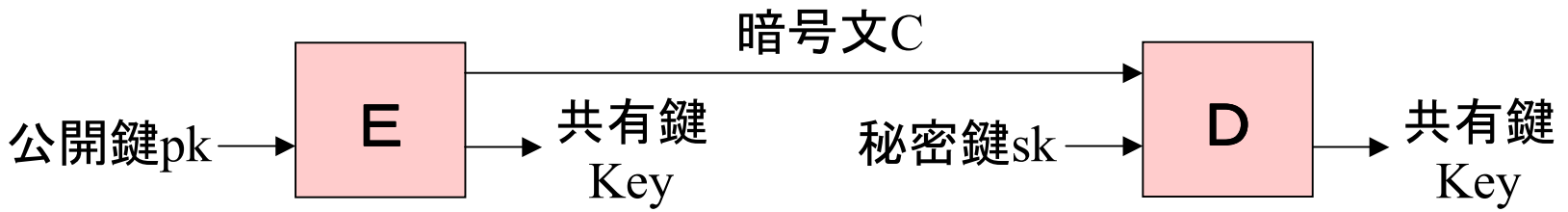
平成14年1月28日

公開鍵暗号評価小委員会
委員　松崎　なつめ

PSEC-KEM暗号

(応募者の主張)

- 応募暗号種別：鍵共有　--図のE,Dと鍵生成を提案
- 証明可能安全性：ﾗﾝﾀﾞﾑｵﾗｸﾙﾓﾃﾞﾙのもとで，最強の安全性を確保.
  (a) 鍵ｶﾌﾟｾﾙ化のIND-CCA2の安全性定義　（by Dr.Shoup）
  (b) ﾗﾝﾀﾞﾑｵﾗｸﾙﾓﾃﾞﾙのもとでEC-CDHへの帰着が証明.
- SW実装：
  鍵生成5.64ms, 暗号化11.09ms，復号10.97ms（Pentium III 600MHz）



暗号評価方法

- PSEC-KEMは,
  - PSEC-2（CRYPTREC2000への応募暗号）の改良として応募された.
  - 本委員会での検討の結果,「新規応募」として評価されることが決まった.
- スクリーニング評価と，参考としてPSEC-2との関係も評価した.

スクリーニング評価

大きな問題は見当たらないが，以下の点が指摘されている．

＜暗号種別に関して＞

暗号技術仕様書には鍵交換のｽｷｰﾑ，自己評価書にはﾊｲﾌﾞﾘｯﾄﾞ暗号における鍵ｶﾌﾟｾﾙ化のｽｷｰﾑとして述べられており，一貫性，対応付けが不明．

＜暗号技術仕様書に関して＞

- ﾌﾟﾘﾐﾃｨﾌﾞ部分に，楕円曲線の推奨ﾊﾟﾗﾒｰﾀが書かれていない．

- ｽｷｰﾑ部分の推奨ﾊﾟﾗﾒｰﾀでどの程度の安全性を達成されるのか不明．

＜自己評価書に関して＞

鍵ｶﾌﾟｾﾙ化の証明可能安全性の定義は妥当であり，証明に不備は見当たらないが，IND-CCA2で最も高いﾚﾍﾞﾙの安全性をもつことが証明されたという主張は誤解を招く．

（参考） PSEC-2（CRYPTREC2000応募）での指摘点に対する改良という観点の評価

項目		PSEC-2		PSEC-KEM
		CRYPTREC2000での指摘	指摘の妥当性	改良有無
ｽｷｰﾑ	1	hLen≅kと書くべきところ，hLen≦kとのみ書かれている（hLen：ﾊｯｼｭの出力ビット数，k：ｾｷｭﾘﾃｨﾊﾟﾗﾒｰﾀ，ﾍﾞｰｽﾎﾟｲﾝﾄの位数のビット数）	妥当	欠落，要修正
	2	rLen≅qLenと書くべきところ，rLen≦qLenとのみ書かれている　（rLen：乱数のビット数，qLen：定義体のビット数）	妥当	仕様変更で該当なし
ﾌﾟﾘﾐﾃｨﾌﾞ	3	記述誤りの存在 楕円曲線ﾊﾟﾗﾒｰﾀの値および楕円曲線の条件の欠如	妥当	欠落，要追加
	4	標数3の体の排除が明記されていない	妥当	解決済み
	5	楕円曲線上要素の第1座標をマスクとして用いると，強秘匿性を損なう可能性があるのではないか.	未検討	仕様変更で該当なし

（参考）PSEC-2との関係および他方法との比較

- PSEC-2との関係：次の理由により別スキームと考えられる．
  - PSEC-2には平文入力がある，PSEC-KEMにはない．
  - カテゴリが異なり，安全性の定義が異なる
  - 共に乱数rを秘匿通信している点は類似しているが，秘匿にPSEC-2は平文が関与しているのに対し，PSEC-KEMは関与していない．
- ECIES-KEM，ACE-KEMとの比較

比較項目		PSEC-KEM	ACE-KEM	ECIES-KEM
処理時間（楕円乗算回数）	Encryption	2	5	2
	Decryption	2	3	1
証明可能安全性	安全性	IND-CCA2		
	モデル	Random Oracle model	Standard model	Random Oracle model
	安全性の仮定	CDH	DDH	Gap-DH