RSA暗号/署名評価の現状報(詳細評価)

平成14年1月28日

公開鍵暗号評価小委員会
委員　太田 和夫

RSA署名,RSA-PSS,RSA-OAEP

- 応募暗号種別：署名，守秘
- 安全性の根拠：n=pq 型素因数分解問題
- 証明可能安全性：n=pq 型素因数分解の困難性との同値性は示せていないが，経験的に安全であると信じられている
- 特長：広く使われている実績，
  広範な観点からの安全性評価
- SW実装情報：Celeron 450 MHz　1 ms (e=3)
  (鍵サイズ 1024 ビット)　　27 ms (CRT使用)

詳細評価

- 次の観点から複数の評価者に評価を依頼:
  - 暗号プリミィティブに関して:我々の把握している情報に見落としはないか／既知の攻撃法が更に進展する可能性はないか
  - 暗号スキームに関して:学界で出版されている証明等に誤りはないか
  - その他:理論として証明されていることが，提案方式に正確に反映されているか

RSA Primitive へのコメント

自己評価書の記述に問題なし（すべての評価者）

- 使用制約についてのコメントあり

  一般的な状況にて

  法の値の共有　　秘密鍵dが小さいとき

  鍵の部分情報から全体の情報の導出

  暗号として使用時

  公開鍵eが小さいとき　　同報通信環境　など

指摘された制約条件はすべて既知であった

RSA 署名(PKCS#1 v1.5)へのコメント

(電子署名法に係る指針に記載された署名方式の1つ)

安全性に対する疑問点の指摘なし(複数回答)

- 証明可能安全性は示されていないことより，RSA-PSSを採用すればよいとのコメントあり
- 提案社が「教科書的RSA」における安全性に対する制約条件から利用を推奨していないため，提案社に「教科書的RSA」の定義を確認したほうがよいとのコメントあり
- 利用状況，方式の寿命等を考慮して議論を行う必要がある

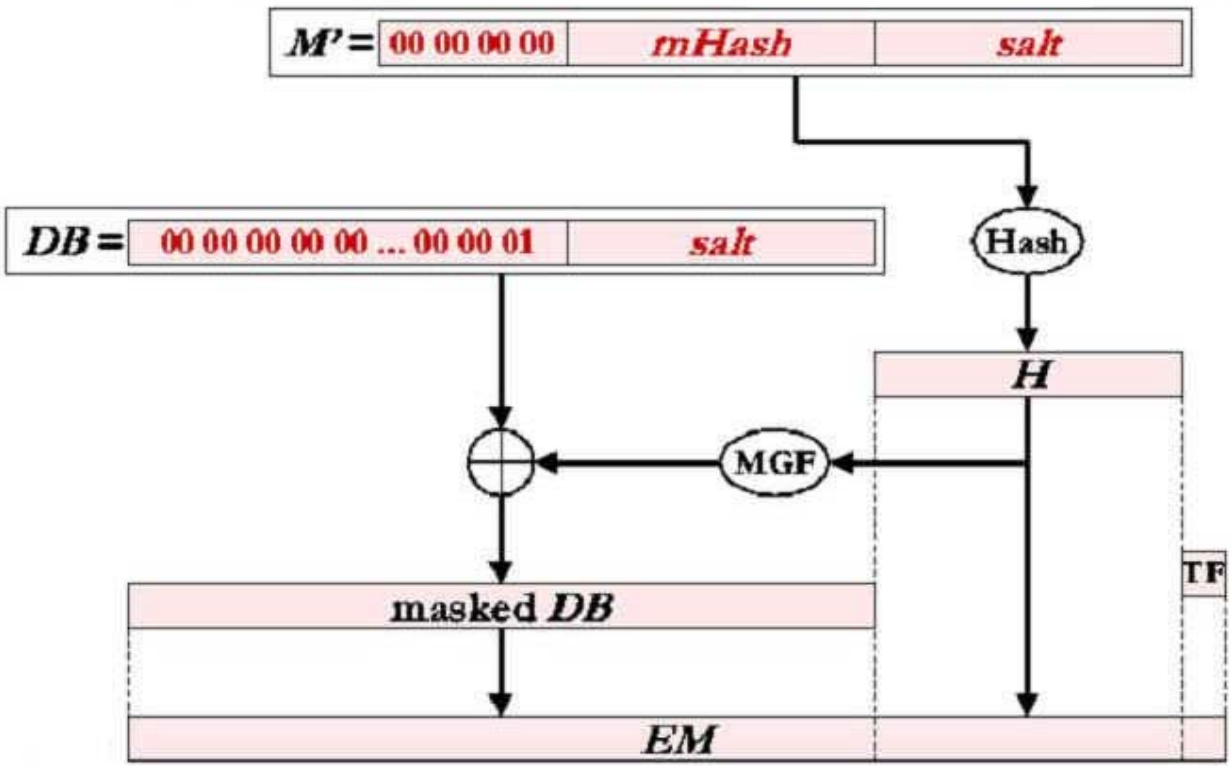
PKCS#1 v1.5 Format

RSA-PSSへのコメント

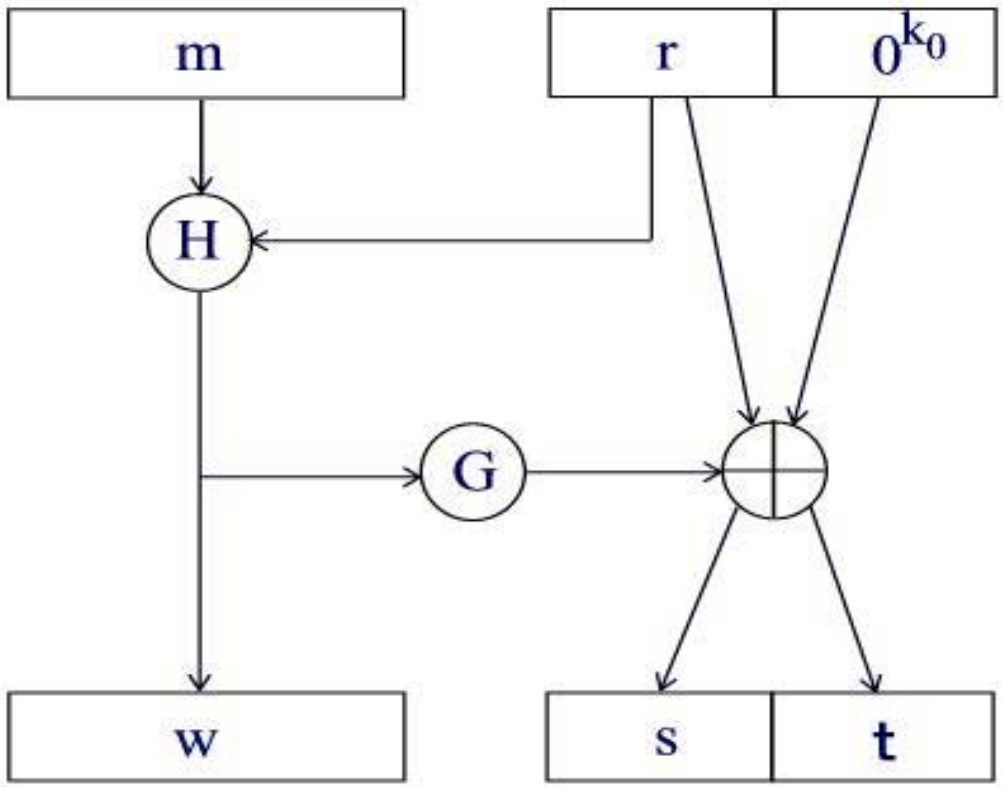
安全性証明は信頼できる (ただしROモデル)

- Jonsson の証明は，hash-id については扱っていないもの，乱数成分(salt)長が可変でそれを悪用する攻撃，エンコード中で用いられる二つの関数に相関がある場合も含めた安全性の評価が行われており，信頼できる
- 仕様変更によって新たに導入された hash-id の悪用の可能性については検討を継続する必要がある（複数の評価者から指摘）
- パラメータの導入により帰着の効率が低下するので法のサイズの選択に注意が必要

PSS Diagram


M' =
00 00 00 00
mHash
salt
DB =
00 00 00 00 00 ... 00 00 01
salt
Hash
H
MGF
masked DB
TF
EM

The Probabilistic Signature Scheme

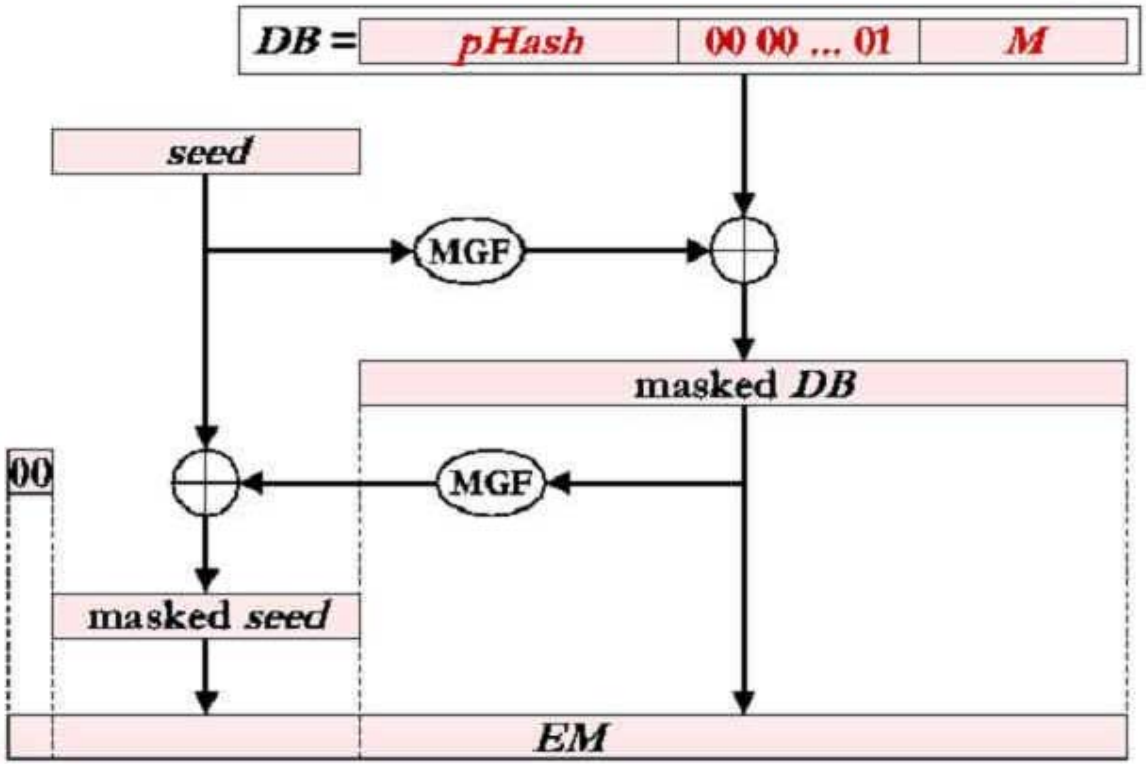


RSA-OAEPへのコメント

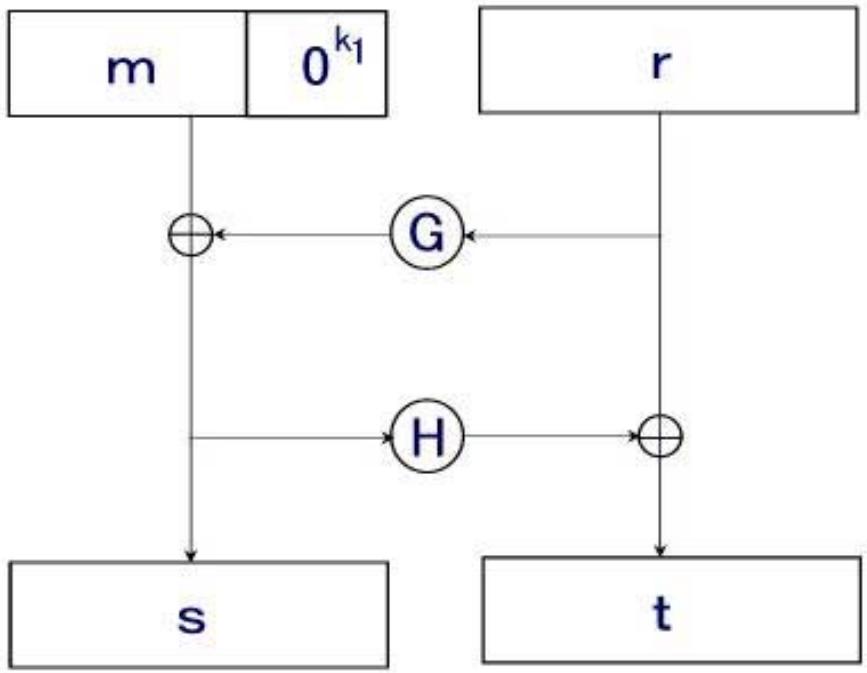
安全性証明は信頼できる（ただしROモデル）

- 提案方式と論文で証明が与えられている記述に若干の相違あり．対応関係を把握して設計パラメータの選択が必要．
- 帰着の効率の観点からRSA-OAEP+を推奨する意見あり（1名の評価者）．
  →検討が必要
- 仕様書のデータ長に記述ミスの可能性あり
  →確認要

OAEP Diagram



Optimal Asymmetric Encryption Padding



今後の課題

- RSA署名 (PKCS#1 v1.5):
  利用状況，方式の寿命等を考慮した議論
- RSA-PSS:
  hash-id の悪用の可能性について継続検討
  帰着効率の低下を考慮した法サイズの選択
- RSA-OAEP:
  設計パラメータの選択
  RSA-OAEP+との方式比較