応募暗号技術の安全性評価について1
エンティティ認証
無限ワンタイムパスワード認証方式（IOTP)

CRYPTREC
Cryptography Research and Evaluation Committees

公募の目的 (公募要項P.4 第5.1節抜粋)

・策定から5年以上が経過し、解析・攻撃技術の高度化及び暗号技術の開発が進展している

・安全性評価のみならず危殆化及び移行対策を含めた適切な暗号選択の支援への要望

・導入コスト、相互運用性、普及度合いなどの評価観点の必要性の指摘

・リストの改訂に必要な技術の追加

CRYPTREC
Cryptography Research and Evaluation Committees

応募暗号に関する留意事項(公募要項P.2 第2.2節抜粋)

・2010年9月までに査読付き国際学会に採択されていること

・第三者が全ての機能を実装可能となる情報が開示されていること

・国内外での評価が可能であること

・評価に際しては、知的財産の利用が無償で行えること

・電子政府リスト策定後3年以内に調達可能なこと

CRYPTREC
Cryptography Research and Evaluation Committees

エンティティ認証(新設)

・電子政府推奨暗号リストに掲載された共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証、あるいは、安全性を計算量的な困難さに帰着できるエンティティ認証

・安全性を脅かす状態としては、なりすましの 成功、セッションの取り換え等を想定

・電子政府推奨暗号リストに掲載されている、あるいは 応募中の共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードのみを利 用している場合には、暗号プリミティブを理想的に安全なものとする

・その他の暗号プリミティブを用いる場合には、暗号プリミティブを理 想化せずに安全性の検証を実施

・提案者はプロトコルの安全性を示す情報を提出し、本公 募における安全性評価では、これらの正当性を検証

CRYPTREC
Cryptography Research and Evaluation Committees

無限ワンタイムパスワード認証方式の受付状況

・応募時点では、提案技術に関して査読付き国際会議における発表はなかった。

・2010年9月までに、事務局では査読付き国際会議への採録は確認できなかった。提案者にも問い合わせを行ったが、採録がないことが確認された。

・以上より、「無限ワンタイムパスワード認証方式」については、応募資格がないことにより、評価を進めないこととする。

CRYPTREC
Cryptography Research and Evaluation Committees