MULTI-S01暗号評価の現状報告（詳細評価）

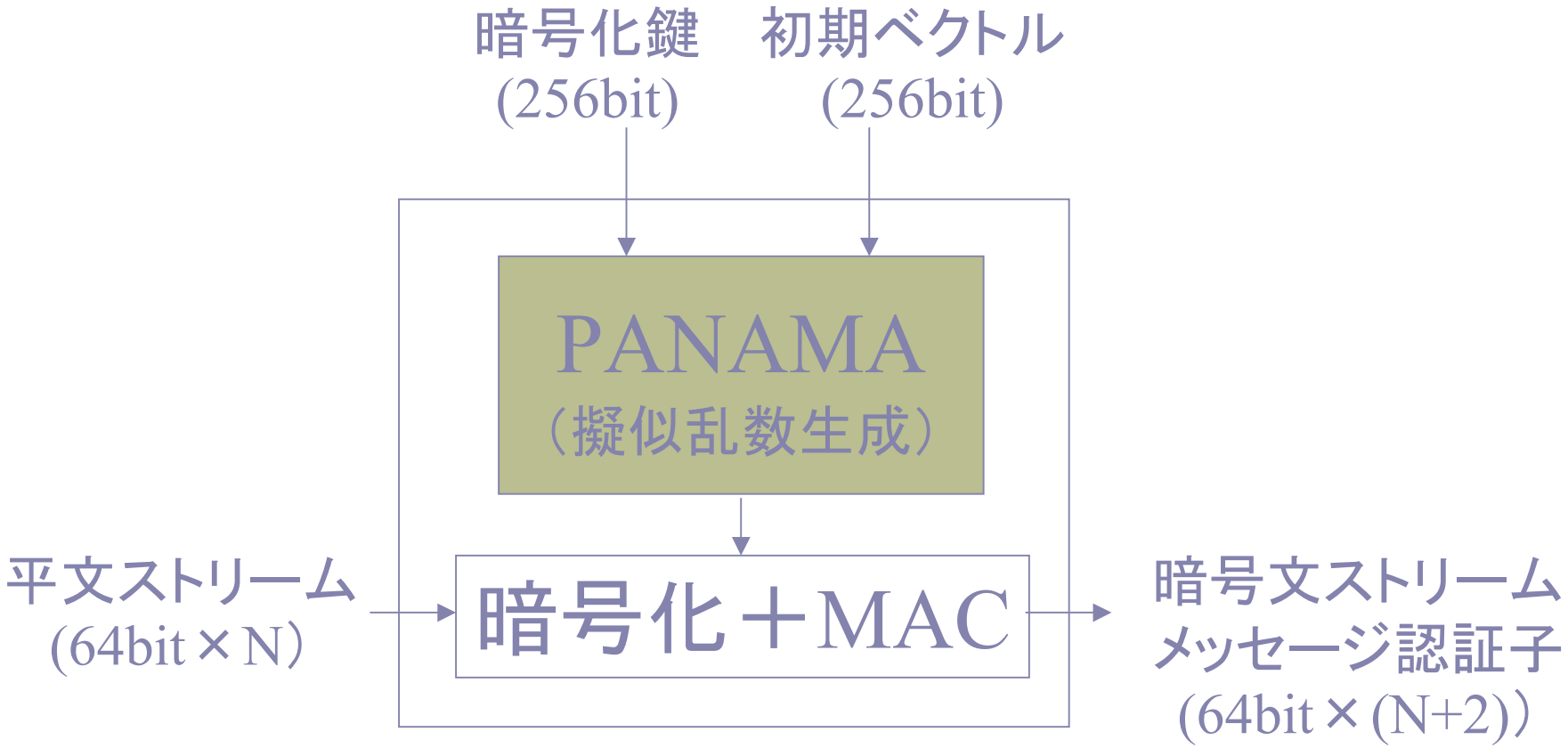
平成14年1月28日

共通鍵暗号評価小委員会
委員　下山　武司、角尾　幸保、荒木　純道

MULTI-S01

- 2000年に日立製作所が発表
- メッセージ認証子(MAC)付ストリーム暗号
- 鍵長256ビット、初期ベクトル256ビット
- 暗号装置内部の擬似乱数生成器として**PANAMA**を利用している。

MULTI-S01の概念図（暗号化）



昨年度の評価

- ストリーム暗号としての安全性については、今のところ問題は見つかっていない。
- 現時点では学会等で厳密な評価が得られておらず、継続的な評価が必要。
- SWにおける処理速度は速いグループ。

(CRYPTREC Report 2000)

評価手順

- 擬似乱数生成部(PANAMA)と利用モードを実現する暗号化部を切り離して評価
- 詳細評価内容

1. MULTI-S01を暗号利用モードとみた評価[2]
2. PANAMAの理論的暗号解析に対する安全性[2]
3. PANAMAの計算機による乱数性検定[1]

([]は評価者数)

1. 暗号利用モードとしての評価

- 暗号部品であるPANAMAの、MULTI-S01装置での利用方法と安全性との関連について評価を行う。
- 本評価ではPANAMAの内部構造までは踏み込まない。

暗号利用モード(評価者1)

- 提案者による「安全性」の定義が不十分。
- 安全性を再定義し評価した結果、MULTI-S01 の暗号化としての安全性及びメッセージ偽造不可能性は PANAMA の性質に帰着可能であろうと考えられる。

暗号利用モード(評価者2)

- 複数のデータストリームに対する暗号化アルゴリズムの定義と認証つきストリーム暗号としての安全性の定義について適当な記述がない。
- 評価者による定義を適用し評価した結果、暗号化としての安全性およびメッセージの偽造不可能性がPANAMAに帰着できることが示された。
- "Carter-Wegman MAC" (より高速で、暗号文にわずかなビットの付加で実現可能な認証付き暗号) と比較した際の長所が見付けられなかった。

2. PANAMAの理論的暗号解析

- MULTI-S01の安全性はPANAMAの影響が大きいことからPANAMA自身の安全性を理論的に評価。
- PANAMAは1998年にDaemenとClappらによって提案された暗号アルゴリズム。ハッシュ関数と擬似乱数生成の2種類を含む。
- MULTI-S01で用いているのは擬似乱数生成部のみ。よってPANAMAの擬似乱数生成部のみ評価する。

理論解析(評価者1)

- 3種類の簡略化 (PANAMA-S1,-S2,-SM, 評価者1は PANAMA-SM が最も本物に近いと考察) を行ない攻撃計算量を計算
- PANAMA-SM は 100 に比例したデータと 2^{65}に比例した計算量で解読可能。(暗号装置の内部状態を復元可能)
- ただし、この攻撃法のPANAMA自身への適用は難しい。

理論解析(評価者2)

- PANAMAの初期ベクトルIV(256bit)に着目。
- 攻撃者が選択した異なる IV を用いて疑似乱数列を生成させた場合について、以下が示された。
  - 同じ疑似乱数列は発生しないこと
  - 差分攻撃、関連鍵攻撃について直ちに分かる弱点はないこと
- 評価が短時間であったこともあり、PANAMA の弱点は見出せなかった。

3. PANAMA の乱数検定

- PANAMAの統計的性質について、NISTのSP800-22により検証

SP800-22とは?

- NISTが公開している、擬似乱数の統計試験ツールとドキュメント
- 試験の出力は189種類の「合格率」と「分布」
- AES選定時に本ツールにより検定

乱数検定（実験結果）

- PANAMA疑似乱数性には特段の欠陥は見当たらないと判断される。

※参考

- NIST の乱数検定 ドキュメントSP800-22に付属している検定プログラム には、少なくとも 2 箇所 (検定項目 DFT、Lempel-Ziv 各々の「分布」評価) で Heuristicなパラメータが真性乱数のそれからずれている可能性があることが判明した。

まとめ

- MULTI-S01の安全性はPANAMAの安全性に帰着可能。
- PANAMAの安全性について、致命的な問題点は現在まで得られてない。
- PANAMAの乱数検定からは、特段の欠陥は見当たらない。