Ｓ０１最新情報

㈱日立製作所
システム開発研究所
古屋　聡一

MULTI－S01

- ストリーム暗号として提案
- 技術的実態はPanama＋操作モード
- 鍵長256ビット
- ソフトウェア、ハードウェアで効率的

Ｓ０１出版物

- 設計段階から国内講演を重ねる：
  1. 古屋聡一, 佐藤尚宜, 高橋昌史, 宮崎邦彦, 宝木和夫, ``メッセージ認証可能なストリーム暗号操作モード," 暗号と情報セキュリティシンポジウムSCIS2000講演予稿集, SCIS2000-A17, 2000.
  2. 古屋聡一, 高橋昌史, 渡辺大, 宝木和夫, ``擬似乱数生成器を使ったメッセージ認証可能な共通鍵暗号の提案," 電子情報通信学会技術研究報告, ISEC2000-8, 2000.
  3. 古屋聡一, 渡辺大, 宝木和夫, ``MULTI-S01のパディングと安全性についての考察," 電子情報通信学会技術研究報告, ISEC2000-68, 2000.
- 平成１２年度ＣＲＹＰＴＲＥＣ応募
- 平成１３年度ＣＲＹＰＴＲＥＣ継続審査（仕様変更などなし）
- WEBで仕様書、自己評価書などを公開

S01最新情報

- 仕様書の改訂(1月27日)
  - 天井関数の定義を掲載しました(和英)
  - 逆元計算の具体的方法を掲載しました(英)
  - Panama初期化スケジュールを掲載しました(英)
  - 鍵ストリーム生成にQを使うことにこだわりました(和英)
  - Qの名前を初期値(initial vector)に統一しました(和英)
  - 「ai+,」の誤記を「ai+4」としました(和)
  - 「二つの目的」→「三つの目的」
  - 「+」、「ー」などの記号の電子的扱いを変更しました(和英)
  - 「C'」などのプライム(ダッシュ)記号を統一しました(和)
  - 復号化処理の変数名(ダッシュ有無)をよりわかりやすくしました(和英)
  - 参考文献にPanamaの原著を加えました(和英)
- SCIS2002にて講演予定