

Message-ID: <3C803E69.F7AEBF05@sdl.hitachi.co.jp>
Date: Sat, 02 Mar 2002 11:52:25 +0900
From: Takaragi Kazuo <takara@sdl.hitachi.co.jp>
To: cryptrec-comment@ipa.go.jp
Subject: (MUGI/MULTI-S01) Comment on Coppersmith's manuscript

CRYPTREC事務局御中

日立製作所システム開発研究所の宝木です。平素より弊社技術に関しましてCRYPTREC活動ならびに詳細評価では大変お世話になっております。

さて、弊社提案の暗号技術、MULTI-S01とMUGIの安全性の議論に関連する技術文書が先日以下のURLにて公開されました。これに関する速報的なコメントを送付させていただきます。ご査収のうえ、今後の評価の参考にさせていただければ幸いです。

URL: <http://eprint.iacr.org/2002/020/>
Title: Cryptanalysis of stream ciphers with linear masking
Authors: Don Coppersmith and Shai Halevi and Charanjit Jutla

弊社コメント

本文書020.pdfは、MULTI-S01で用いる擬似乱数生成器Panamaと、弊社提案のストリーム暗号MUGIの安全性に関連する話題です。より具体的には本文書で攻撃対象として扱う構造をPanamaとMUGIでは有しています。最終的なわれわれの判断は、今回の攻撃手法は現状われわれの自己評価、ならびに既知の安全性評価の範疇であり、新しい技術的欠陥の記述ではない、と捉えます。また、海外の研究者との議論分析も行いましたがほぼ同じような意見を得ております。

しかしながら、いくつかの技術観点は重要であり、今後も本文書を解析のうえ、将来のMULTI-S01、MUGIの安全性評価へ反映させていきます。

詳細な内容ですが、今回提案された攻撃の概要は、出力列のみからなるバッファ値の記述（確率的、代数的問わずあらゆるかたちで）をし、バッファの構造にあわせてこれらを組み合わせるものです。また、攻撃にはWalsh-Hadamard変換を使うことで必要なデータの削減を期待できます（しかし、必要なメモリや計算量は増加します）。この攻撃は特にSNOWストリーム暗号に効果的で、鍵の全数探索よりも少ない計算量で攻撃可能であることが主張されています。また、攻撃の対象となる暗号として、次の構造をもつことと主張しています：内部状態が、線形、非線形な部分に分割でき、非線形な部分が乱数と識別可能であってこれらが線形に作用しあい、線形に出力を生成するもの。

MUGI、Panamaはどちらもこの構造をもったアルゴリズムです。しかし、Daemenによる安全性評価[1]やMUGIの自己評価[2]はどちらも次のような攻撃を主に考慮しつつ設計を行っています：非線形な部分から可能な近似の条件を決定し、可能な近似を組み合わせることで確率や代数次数が安全な方向へ飽和する。また、攻撃適用の容易性からPanama、MUGIともに非線形部分の線形近似[3]には詳細に評価を行い、最終的に出力列のみからなる有意な線形近似（特性確率）は構築できない、と結論付けています。

今回の攻撃手法はひじょうに汎用的な記述をしている、とも考えます。例えば、DESのようなFeistel構造において、「F関数に対して任意の性質を考え、これらを組み合わせることで平文と暗号文のみからなる相関を使った攻撃」と記述することはできます。しかし、現状の情報では、これが実際の攻撃手法の指摘とは必ずしもならないと考えます。

しかし、当然ながら将来もずっとPanamaやMUGIに対する解読法がまったく存在しない、と言えるものではありません。我々は今回の攻撃モデルを改めて検討し、将来の新しい安全性評価手法やアプローチを追及する所存です。

事務局のみなさま、ならびに委員のみなさまにおかれましては、上記弊社意見をご理解のうえ、今後の評価活動の参考にさせていただければ幸いです。

参考文献

- [1] J.Daemen, "Cipher and hash function design strategies based on linear and differential cryptanalysis," Doctoral Dissertation, Marc 1995, K.U. Leuven.
- [2] 株式会社日立製作所, "疑似乱数生成器MUGI, 自己評価書" CRYPTREC提案暗号アルゴリズム, 2001年9月25日, 2001.
- [3] 松井 充, "DES 暗号の線形解読法(I)," 1993年暗号と情報セキュリティシンポジウム, SCIS講演予稿集, SCIS93-3C, 1993.

宝木 和夫

(株)日立製作所システム開発研究所
第7部(セキュリティシステム研究部)
〒244-0817 横浜市戸塚区吉田町292
TEL (045)860-3072 FAX (045)860-1662
E-mail: takara@sdl.hitachi.co.jp
URL: <http://www.sdl.hitachi.co.jp>
