Rijndaelに関して

概要(和文)
Rijndaelを、ここ一年（2001年度）以内に
日本の電子政府用暗号として
採用することには賛成しない。

現在まで、決定的攻撃法が見つかっているわけではなく、
今日までの解析結果は、その安全性を保証している。
しかし、提案されて3年たらずであり、最低でもあと１年、
できれば２、３年は解析を続けるべきである。

特に鍵生成アルゴリズムに対する解析は、
最新の解読手法を考慮してもっと検討すべきであろう。

英文アブスト
Japanese goverment should not
use Rijndael within one-year,
though no serious cryptgraphic problem
is discovered yet.

We should do further evaluation of Rijindael
in one more two years.
In particular, key-scheduling algorithm
shall be investigated.

詳細報告
Rijndael[AESrij]を、ここ一年（2001年度）以内に
日本の電子政府用暗号として
採用することには賛成しない。

NISTは、AESワークショップをはじめとする
公開報告にもとづき、
一連のAES選定、および
AES-winnerとして最終選定した理由を
報告書で報告している[AESr2]。

具体的に論文で発表されている攻撃としては
5,6段Rijindaelに[BN2000]: Square,改良Square,不可能差分、攻撃。
しかし、いずれも6段までの攻撃。
Collision attack[GM2000]:192ビット鍵および256ビット鍵
２３２の選択平文を用いて７段まで解読可能
Square attack[Lucks2000]:192ビット鍵および256ビット鍵、
２３２の選択平文を用いて７段が解読可能[?]。
Square attack(改良版)[Fer2000]、128ビット鍵は７段まで、
256ビット鍵は８段まで解読可能.
(注意　ただしこの解読法で必要な選択平文数は、ほぼ全数にあたる.)
Related key attack（関連鍵攻撃)[Fer2000]: 256ビット鍵が９段まで解読可能.

このように現在まで、
フルスペックのRijndaelに対して
決定的攻撃法が見つかっているわけではなく、
今日までの解析結果は、その安全性を保証している。
ただし、Murphy-Robshowの観察のように、未だ
Rijndaleの構造に暗号論的弱点が潜む可能性を

疑う研究者もいる[MR1,DR,MR2]。

また、AES報告書[AESr2]では、
Rijndaelは適度セキュリティマージンを持つとしているが、
他のAES候補(e.g. Serpent)と比較すると、Rijndaelのセキュリティマージン
は相対的に低く、速度を込めたセキュリティマージンの議論が必要とする
研究者もいる。

提案されて3年たらずであり、最低でもあと１年、
できれば２、３年は解析を続けるべきである。
ただし、Rijndaelは、それ以前から設計者らが
提案していたブロック暗号の改良版としては、
SHARK[Shark], SQUARE[Square]などもっと長い歴史をもつ。

最近提案の日本１２８ビット暗号は、Rijndael以上の解析が必要であろう。
日本提案の電子政府採用には、最低でも３年は慎重に
検討すべきである。

特に鍵生成アルゴリズムに対する解析は、
もっと検討すべきであろう。
（これは日本提案の１２８ビットブロック暗号にも共通の課題である[Aoki].）

また、同じ構造を強化したとされるHierocrypt@東芝[CRYPTREC-web]との
比較も重要である。本当にHierocryptは、Rijndaelよりも
暗号論的に強化されているのか、あきらではない。
Murphy-Robshowの指摘も含めて、最低あと一年は
電子政府利用にむけて、慎重に解析を続けるべきである。

参考文献

[AESrij] AES proposal: Rijndael,
AES algorithm submission, September 3, 1999,
from http://nist.gov/aes .

[AESr2] J.Nechvatal,et al.,
Report on the Development of the Advanced Encryption Standard (AES),
National
Institute of Standards and Technology, October 2,2000,
r2report.pdf from http://csrc.nist.gov/encryption/aes/

[BK2000]
E. Biham, N. Keller: Cryptanalysis of Reduced Variants of Rijndael
http://csrc.nist.gov/encryption/aes/round2/conf3/papers/35-ebiham.pdf

[Shark]V.Rijmen, et al., The Cipher SHARK,
3rd Fast Software Encryption, 1996, LNCS 1039, pp.99-112,
Springer-Verlag, 1996.

[Sqaure]J.Daemen, L.Knudsen and V.Rijmen, The Block Cipher Square,
4th Fast Software Encryption,
FSE'97, LNCS 1267, pp.28-40, Springer-Verlag, 1997.

[GM2000]H.Gilbert and M.Miner, A collision attack on 7 rounds of Rijndael,
in The Third AES Candidate
Conference,printed by the National Institute of Standards and Technology,
April 13-14,2000,pp.230-241.

[Lucks2000]S.Lucks,Attacking Seven Rounds of Rijndael Under 192-bit and 256-bit Keys,
in The Third AES Candidate Conference,
by the National Institute of Standards and Technology, Gaithersburg, MD, April 13-14,2000,pp.215-229.
AES3Proceedings.pdf from http://csrc.nist.gov/encryption/aes/

[Sugita2000]
Sugita et al.
AES3Proceedings.pdf from http://csrc.nist.gov/encryption/aes/

[Fer2000]
N.Ferguson,et al., Improved Cryptanalysis of Rijndael,
in the preproceedings of the Fast Software
Encryption Workshop 2000, April 10-12, 2000.

[BK2000]
E. Biham, N. Keller: Cryptanalysis of Reduced Variants of Rijndael
http://csrc.nist.gov/encryption/aes/round2/conf3/papers/35-ebiham.pdf

[MR1]
"New observations on Rijindael"
by Sean Murphy and Matt Robsow (7th Aug. 2000)
from http://nist.gov/aes .

[DR]
Answer to "New observations on Rijindael" (11th Aug. 2000)
J. Daemen and V.Rijmen
from http://nist.gov/aes .

[MR2]
"Further comments on the strucutre of Rijindael"
by Sean Murphy and Matt Robsow (17th Aug. 2000)
from http://nist.gov/aes .

[Une1]
DPS97-J-16 宇根 正志 AES (Advanced Encryption Standard) について 97/11

[Une2]
DPS 98-J-21 宇根 正志 最近のAESを巡る動向について 98/09

[UO]
金融研究
18巻2号 宇根 正志
太田 和夫 共通鍵暗号を取り巻く現状と課題 —DESからAESへ—
99/04

[Aoki]
青木 ほか
128ビットブロック暗号の安全性能比較 Proc. SCIS2001,
(another version from ISO/SC27/WG2-Japan)