TripleDESに関して

概要(和文)

TripleDESは、電子政府用の機密保護暗号に利用することには
問題ないと考える。

ただし、two-key TDESではなく、
three-key TDESが推奨される。

電子政府が、より高速なソフトウエア暗号を必要とするならば、
他の６４ビットブロック暗号を選択することもできるであろう。

暗号論的安全性に関しては、
最近の解読技術（高階差分、まるめ差分、鍵スケジュール攻撃など)
に対する論文がほとんどない点、気になるところである。
多くの最新攻撃は、AES候補に対してであり、
TDESに対しての効果は論じられていない。
以上

概要(英文)

No public problem is found for using TripleDES
as Japanese electronic goverment's encryption.
TDES with three-key might be better than TDES with two-key
in the use of Japanese electronic goverment's encryption.

If goverment need a more faster encryption algorithm than TDES,
alternative candidates could be exsisting.
No paper is published that discusses
recent cryptoanalysis (e.g. higher differential, truncated diff.)
against TDES. This does not imply the security of TDES,
so we should do further evaluation of cryptographic security of TDES
against recent attacks in future.

詳細報告

TripleDESは、電子政府用の機密保護暗号に利用することには
問題ないと考える。

(Single)DESに対する代表的攻撃である
差分解読[BS]や線形解読[Ma]は、段数を重ねた
TripleDES(with two/three-keys)には脅威ではない。
しかし、中間一致攻撃や鍵相関攻撃などにより、
実質の鍵長が２倍３倍とはならないことには注意がいる。

鍵長
ただし、two-key TDESではなく、
three-key TDESを利用すべきである。
機密保護に利用するか、ハッシュ関数的に利用するかでも、
差があるが、two-keyでも、その実質鍵は112ビットまでには
至らない場合があることに注意すべきである。
一般に、ハッシュやＭＡＣの場合、誕生日攻撃などの

衝突探索が脅威となり、実質鍵長が(three-keyでも)
みかけの鍵長よりも短くなる[vOW99]。

このような攻撃は、ソフトウエア上だけでの
攻撃に対しては、現実的脅威ではなく、
ハードウエア攻撃に対してもコストの面で
割にあわないというレポートもある[KM,TOK].
しかし、Electronic Frontier Foundation"Cracking DES"[EFT]
では、予想以上にsingleDESの解読チップが安いコストで実現可能と
報告されている。
[EFT]と[vOW99]とを合わせたTDES攻撃チップの実現コストは
未だ算出されていない。

実装速度
DESは本来HW用に設計され、SW実装では速度に問題があるといわれる
場合もある。しかし，DESは歴史が古く、高速SW実装も研究されており、
絶対速度として遅い、と考えるには誤解がある。
ただし、（ソフトウエア）処理速度の面では、
後発のアルゴリズムの方が数倍高速であることは
事実であろう。

TDES 対　最新暗号
電子政府が、より高速なソフトウエア暗号を必要とするならば、
他の６４ビットブロック暗号を選択することもできるであろう。
しかし、以上（TDES）より高速なアルゴリズムで
TDES以上の安全性・信頼性のある後発（ブロック）
暗号アルゴリズムは、ないのではないか。

暗号論的安全性に関しては、
最近の解読技術（高階差分、まるめ差分、鍵スケ
ジュール攻撃など)
に対する論文がほとんどない点、気になるところである。
鍵スケジュール攻撃に関しては、[KSW]において、
TDES(with three-key)がTDES(with two-key)
よりも弱い攻撃環境があることが指摘されている。

多くの最新攻撃は、AES候補に対してであり、
TDESに対しての効果は論じられていない。
しかし、否定的な論文が報告されているわけでもない。
TDESも、あと5年以上は、利用されると考えられる。
もし、電子政府で利用するのであれば、
こうした、最新の攻撃に対する安全性も
今度検討していくべきであろう。

特にTDES（や６４ビットブロック暗号）の普及度を考えると、
128ビット（192ビット）鍵長64ビットブロック暗号の
ハードウエア解析の現実性を、コスト面までこめて、
検討すべきであろう。

参考文献
[EFT] Electronic Frontier Foundation
"Cracking DES", O'reilly (May 1998).

http://www.eff.org

[X9.52]
American National Standards Institute,
"X9.52-1998,Triple Data Encryption Algorithm Modes of Operation,"1998.
(from NIST-web).

[NISTdes]
National Institute of Standards and Technology,
"Data Encryption Standard," FIPS 46-3,1999.

[TOK] 谷口,太田,大久保：Triple DESを巡る最近の標準化動向について,
金融研究弟18巻別冊第1号,日本銀行金融研究所,1999
http://www.imes.boj.or.jp/security/

[UO] 宇根,太田：共通鍵暗号を取り巻く現状と課題 —DESからAESへ—,
金融研究弟18巻第2号,日本銀行金融研究所,1999
http://www.imes.boj.or.jp/security/

[KM] K.Kusuda and T.Matsumoto,
"A Strength Evaluation of the Data Encryption Standard", IMES
Discussion Paper, No.97-E-5,
Institute for Monetary and Economic Studies, Bank of Japan,1997.
http://www.imes.boj.or.jp/security/

[Lucks]S.Lucks, Attacking Triple DES,
Proc. of Fast Software Encryption '98, LNCS,
Vol.1372,1998,pp.239-253.

[vOW90] P.C.van Oorschot and M.J.Wiener,
A known plaintext attack on two-key triple encryption, Advanced
in Cryptology Proc. of EUROCRYPT090, LNCS, Vol.473, Springer-Verlag,
1990,pp.318-325.

[vOW96]P.C.van Oorschot and M.J.Wiener,
Improving implementable meet-in-the-middle attacks by
orders of magnitude,
in Cryptology Proc. of CRYPTO'96,
LNCS 1109, Springer-Verlag, 1996,pp.229-236.

[vOW99]P.C.van Oorschot and M.J.Wiener,
Parallel collision seach with cryptanalytic applications,
J.of Cryptology, Vol. 12 No.1 Winter 1999.

[BS]E.Biham and A.Shamir, Differential Cryptanalysis of the Full 16-round
DES, Advances in
Cryptology Proceedings of CRYPT092, LNCS, Vol.740, Springer-Verlag,
1993,pp.487-496.

[Ma]M.Matsui, Linear Cryptanalysis Method for DES Cipher, Advances in
Cryptology ?Proceedings of
EUROCRYPT93, LNCS, Vol.765, Springer-Verlag, 1994,pp.386-397.

[KSW]J.Kelsey, B.Schneier, and D.Wagner, Key-Schedule Cryptanalysis of IDEA,

G-DES, GOST, SAFER,
and Triple DES, Advances in Cryptology CRYPT96, LNCS, Vol.1109, pp.237-251,
Springer-Verlag,1996.