ＳＨＡ－１を利用した疑似乱数生成に関して

概要（和文）
SHA-1を利用した擬似乱数生成に関して

FIPS規格の擬似乱数生成器(with SHA-1)を
電子政府で利用することには問題ないと考える。

ただし、適用する暗号方式（電子署名）で、
ランダムオラクルの実現として、
このSHA-1ベースの擬似乱数を利用すると、
理論的証明の仮定が成立しないことに注意すべきである。

しかし、擬似乱数の利用される応用にもよるが、
実装環境の制限等により、SHA-1ベースになっても、
現状問題はないといえる。
できれば、今後１，２年内に規格化されるであろう次世代ＳＨＡを
利用したほうが望ましい。

英文
PRG with SHA-1(FIPS-186)

No problem has been found in
Japanese electronic goverment's use
of FIPS-186 with SHA-1 as pesudo-random generator.

We should note that
the pseudo-random generator is not random-oracle,
so the security argument for cryptographic schemes
in random-oracle-model does not always hold
with the pseudo-random generator.

If Japanese electronic goverment still have time,
it would be better to choose
the advanced SHA with longer size,
which is decided within a few years.

==========
詳細（和文）

SHA-1を利用した擬似乱数生成に関して

FIPS規格の議事乱数生成器(with SHA-1)を
電子政府で利用することには問題ないと考える。

ただし、SHA-1自身を電子署名用ハッシュ関数に
利用する場合には、誕生日攻撃により2**80程度の計算量で
改ざんの危険性がある。これは、今日最低の安全性ラインである。
ただし、これはSHA-1のアルゴリズム自体の問題というよりも、
160ビットハッシュ関数共通の問題である。
NISTが現在検討中のより長い出力の次世代ＳＨＡは
この問題を解決できる。

SHA1(乱数生成)

擬似乱数としてSHA-1を利用した場合（FIPS）、
誕生日攻撃がそのまま、脅威になるとは限らない。
しかし、電子署名や機密保護暗号スキーム(e.g. OAEP)では、
安全性の理論的証明に、乱数生成器が理想的にランダムであることを
仮定するものもある。こうした場合。、自然に衝突一致困難性が
要求され、SHA-1では、安全性の証明がうまく動作しないばあいもある。

FIPS-186では、電子署名規格ＤＳＡの個人秘密情報生成と
署名文書ごとに利用する秘密乱数とにSHA-1ベースの擬似乱数生成を
規定している。理論的安全性（ランダムオラクルモデル）で障害となるのは、
後者の署名文書ごとに対する秘密乱数に対する利用である。
DSAの安全性は（現在まで）ヒューリスティックであるが、
多くの（ランダムオラクルモデル下で）証明可能安全と主張している
署名・暗号方式は、この理想的ランダム性と擬似ランダム性との
格差に注意がいる。
ただし、多くの実用的（証明可能安全な）署名方式で、
この理想的ランダム性と擬似ランダム性との差が
実際の攻撃に即むすびつくことかどうかは
知られていない。

☆最近 DSAの問題点が議論されているが、
　これはSHA-1の性質に起因するものではない、とのことである([Don])。

SHA-1(FIPS-180-1)は、その前身であるSHA(FIPS-180)
のを改良したもとのされている。
この改良の理由は、Preneelの学位論文で
論じられているとされている[Handbook of Applied Cryptography]が、
今回Preneelの学位論文は入手できず、調査していない。
また、SHA-1は、Pentium用の並列処理に適した
アルゴリズムであるという論文[Eurocrypt]もある。
これらがNIST/NSAが意図的に改造したかどうかは定かでない。

SHA-1を利用した擬似乱数生成の統計的性質に関しては、
昨年度NISTより評価レポートが公開されている。
（FIPS-180-1規格時点で、どの程度の評価が行われていたかは不明である。）
ここでは、次の１６個の統計検定が議論されている。

1 Frequency (Monobit) Test
2 Frequency Test within a Block.
3 Runs Test
4 Test for the Longest Run of Ones in a Block
5 Binary Matrix Rank Test
6 Discrete Fourier Transform (Spectral) Test
7 Non-overlapping Template Matching Test
8 Overlapping Template Matching Test
9 Maurer's "Universal Statistical" Test
10 Lempel-Ziv Compression Test
11 Linear Complexity Test
12 Serial Test
13 Approximate Entropy Test
14 Cumulative Sums (Cusum) Test
15 Random Excursions Test
16 Random Excursions Variant Test

このNISTのレポートでは、特にFIPS-180-1 (with SHA1) に
統計的問題点は指摘されていない。

擬似乱数の利用される応用にもよるが、
実装環境の制限等により、SHA-1ベースになっても、
現状問題はないといえる。
だたし、実装環境の障害がなければ、今後１，２年内に規格化されるであろう次世代ＳＨＡを
利用したほうが電子政府用の暗号システムとしては望ましいと考える。
実装環境に制限がある場合には、SHA-1（あるいはDES）ベースの
FIPS-186擬似乱数生成法でも、生成する擬似乱数の長さや回数を
考慮すれば、安全に利用できるといえる。

文献

[HAC]
Handbook of Applied Cryptography
from http://www.cacr.math.uwaterloo.ca/hac/

[NIST]
"A statistical test suite for random and pesudorandom
number generators for cryptographic applicaitons"
(revise Dec.2000)
NIST-report SP800-22.pdf from http://csrc.nist.gov/encryption/

[Don]Personal comm. with DonJohnson@Certicom (Feb.2001)