ＤＳＡ 署 名 評 価 報 告 書

２００１年度

日本電信電話株式会社

岡本 龍明

阿部 正幸

DSA 署名評価報告書

1 はじめに

本報告書では、DSA 署名 [1] の安全性について、現在までに知られている結果について報告する。

DSA 署名に対する攻撃法としては、FIPS PUB 186-2 [1] の Appendix 3 に記述されている疑似乱数生成方法について、Bleichenbacher により指摘された弱点がある。さらに、公開鍵（パラメータ）を変更することによる攻撃方法が Vaudenay により指摘されている [2]。

一方、個々の攻撃法ではなく、基本的な仮定の下で安全性を証明することが最近重要視されているが、DSA 署名についてはそのような証明は報告されていない。

本報告書では、上記で述べた攻撃法や安全性証明の現状について述べる。

2 FIPS PUB 186-2 Appendix 3 の乱数生成について

2.1 概要

Appendix 3.1 では、$(0, 2^{160} - 1)$ の出力域を持つ疑似乱数生成器 G を用いて秘密鍵 x を生成する手順を規定している。秘密鍵 x は $(0, q-1)$ の一様分布に従って生成されるべきである。同手順の Step 3-c によれば、x は $t, XVAL$ を乱数種として

$$x = G(t, XVAL) \bmod q$$

のように生成される。q は $(2^{159} + 1, 2^{160} - 1)$ に入る素数なので、G の出力が一様分布であると仮定すると、$\bmod q$ の折り返し効果によって、x が $(0, 2^{160} - 1 - q)$ に入る確率は $(2^{160} - q, q)$ に入る確率の二倍になってしまう。この x の分布の偏りは $q = \frac{3}{4} \cdot 2^{160}$ の時最大となり、その一様分布からの Statistical Distance は $\frac{1}{3}$ となる。

同様の現象が乱数 r, k の生成時にも発生する。

2.2 対策

D. Bleichenbacher の指摘によって、現在 FIPS PUB 186-2 [1] には Change Notice 1 が付記されており、上記問題点に対する修正が図られた。Change Notice 1 の Random Number Generation によれば、x は

$$x = G(t, XVAL)||G(t, XVAL') \bmod q$$

のように生成される。乱数 r, k の生成も同様に修正されている。

2.3 効果

上記体策により、mod q による折り返し効果の影響は無視できる程度に小さくなり、G を一様分布と仮定すると、 x の分布は $(0, q-1)$ の一様分布と統計的に判別不可能になる。また、同対策は既存の DSA の署名生成、検証に影響せず、interoperability に影響を与えない。

3 Vaudenay の攻撃法について

3.1 攻撃の概要

文献 [2] で指摘されている攻撃方法を紹介する。

H を DSA 署名で用いるハッシュ関数とすると、H の出力サイズと q のサイズは、いずれも 160 ビット程度となる。このとき、

$$H(m) \equiv H(m') \pmod{q}$$

を満たすとき、文書 m に対する正規の署名 s が、別の（偽造）文書 m' に対する署名となる。つまり、署名の偽造に成功することになる。そこで、様々な偽造文書 m' に対して $H(m) - H(m')$ が素数かどうかを検査し、素数となるとき、その値を（偽造された）q として公開パラメータ q を変更する。

さらに、p, q の生成法に準拠した攻撃法も指摘されている。また、上記の攻撃法以外に公開パラメータ g に 0, 1 や $y^{\alpha} \bmod p$ などの特殊な値を用いる攻撃方法も指摘されている。

3.2 攻撃の効果および対策

上記攻撃は、公開パラメータに対して、信頼できる認証局などの証明書を付与することにより容易に解決できる。さらに、個々の公開鍵に対する証明書を付与する際に、公開パラメータも公開鍵の一部として証明書の証明対象とすることにより上記攻撃法を避けることができる。

4 安全性の証明

現在のところ、暗号学的に妥当とされるモデルに基づいた安全性の証明は発表されていない。一部の mod$q$ 演算をハッシュ関数で置き換えた場合はランダムオラクルモデルで安全性の証明が可能であるが、そのような証明はオリジナルの DSA の安全性に関して何ら根拠を与えるものではない。

5 おわりに

本報告書では、DSA 署名 [1] の安全性について、現在までに知られている結果について報告した。

FIPS PUB 186-2 [1] の Appendix 3 の疑似乱数生成方法に関する Bleichenbacher により指摘された弱点は、既に [1] の Change Notice (October 5, 2001) により修復されている。

また、公開鍵（パラメータ）を変更することによる Vaudenay 攻撃法 [2] は、標準的な PKI による証明書などを用いることにより容易に解決できると考えられる。

一方、DSA 署名については、何らかの妥当なモデルや仮定の下での安全性証明は報告されていない。しかしながら、現在までに報告されている攻撃法はいずれも実用的な利用環境では特に問題があるとされているものはなく、現時点では DSA 署名の安全上の問題は無いと思われる。

参考文献

[1] Federal Information Processing Standards Publication, FIPS PUB 186-2, Digital Signature Standard (DSS), U.S. Department of Commerce / National Institute of Standards and Technology (January 27, 2000).

[2] Vaudenay, S.: Hidden Collisions on DSS, Proc. of Crypto'96, LNCS 1109, Springer-Verlag, pp.83–103 (1996).