2004 年 8 月 17 日

梅署名

以下に出てくる数は全て自然数である。

r , k_1 , k_2 は乱数。

公開鍵･秘密鍵生成条件

$k_1<n$, $k_2<n$, $r<n$, $k_1^2>n$, $k_2^2>n$

かつ

$gcd(r,n)=1$

【公開鍵】 n $r^2(\ mod\ n)$ $k_1^2(\ mod\ n)$

【署名生成】 送信者は乱数 k_2 を生成し、
以下の計算によって署名 $(s_1\ ,\ s_2\ ,\ k_2^2\ ,\ k_1k_2)$ を生成する。
ただし、平文を M、ハッシュ関数を h とする。

$$m=h(M)$$
$$s_1=k_1r^{(2m+1)}+k_2r^{-(2m+1)}\ (mod\ n)$$
$$s_2=k_2r^{(2m-1)}+k_1r^{-(2m-1)}\ (mod\ n)$$

【署名検証】 受信者は公開鍵 r^2 , k_1^2 を利用して、以下の等式が成立するか否かを検証する。

$$s_1s_2=k_1k_2r^{(4m)}+k_2^2r^{-2}+k_1^2r^2+k_1k_2r^{(-4m)}\ (mod\ n)$$
$$\frac{s_1}{s_2}=\frac{(s_1s_2)}{s_2^2}\Leftrightarrow s_1(s_2^2)=s_2(s_1s_2)$$

つまり、

$$s_1(k_2^2r^{(4m-2)}+2k_1k_2+k_1^2r^{-(4m-2)})$$
$$=s_2(k_1k_2r^{(4m)}+k_2^2r^{-2}+k_1^2r^2+k_2k_2r^{(-4m)})\ (mod\ n)$$

【安全性】 mod n の平方根を求めることが困難なことによる。
したがって、n は素数がいいかもしれません。
n が素数でなくても署名は行えます。

【利点】 べき乗回数がハッシュ値の値なのでべき乗回数が少なくなる。

執筆者 梅どぶろく◆21Da3ggG3M