

Chaum's Blind Signature & Untraceable e-Cash

Pre-requisites: notes for RSA algorithm.

Public Key: $pk = (n, e)$

Secret Key: $sk = (n, d)$

Blind Signing:

Scenario: Alice wants to have Bob's signature on M .

Step1: Alice generates random number r

Compute $B = (r^e M) \bmod n$ (M is hidden in B)

Step2: Bob signs on B

Compute $U = B^d \bmod n$

Step3: Alice unbinds the signature

Calculate i that $(ir) \bmod n = 1$ (the modular inverse of r)

$S = (Ui) \bmod n = (U \bmod n \cdot i \bmod n) \bmod n$

S is the blind signature on M

Correctness:

$$ir = kn + 1 (k \in \mathbb{Z}^+), i = \frac{kn + 1}{r}$$

$$S = (Ui) \bmod n = (B^d \bmod n \cdot \frac{kn + 1}{r}) \bmod n = (((r^e M) \bmod n)^d \bmod n \cdot \frac{kn + 1}{r}) \bmod n$$

$$S = ((r^{de} M^d) \bmod n \cdot \frac{kn + 1}{r}) \bmod n = ((r^{de} M^d) \bmod n \bmod n \cdot \frac{kn + 1}{r} \bmod n) \bmod n = (r^{de} M^d \frac{kn + 1}{r}) \bmod n$$

$$S = (r^{de-1} M^d (kn + 1)) \bmod n = (r^{de-1} M^d) \bmod n = (r^{de-1} \bmod n \cdot M^d \bmod n) \bmod n$$

$$\because de \bmod(\varphi(n)) = 1,$$

$$\therefore de = l\varphi(n) + 1 (l \in \mathbb{Z}^+)$$

$$r^{de-1} \bmod n = r^{l\varphi(n)} \bmod n = (r^{\varphi(n)} \bmod n)^l \bmod n$$

$$\because |r| < |p|, |r| < |q|,$$

$$\therefore \gcd(r, n) = 1 \text{ (fac}(n) = \{1, p, q, n\})$$

$$\therefore r^{\varphi(n)} \bmod n = 1 \text{ (Euler's Theorem)}$$

$$\therefore r^{de-1} \bmod n = 1, S = (M^d \bmod n) \bmod n = M^d \bmod n$$

(same as a regular RSA signature!)

Double-spending detection in e-Cash:

Each e-Cash coin contains two shares – S_0 and S_1 .

S_0 or S_1 solely will not reveal payer's identity, but the combination of two shares will.

Suppose S_0 is a sequence of random bits, u is the bit string of payer's real identity, then $S_1 = u \oplus S_0$.

Due to the reversibility of XOR, $u = S_1 \oplus S_0$.