Anonymity of undeniable signatures

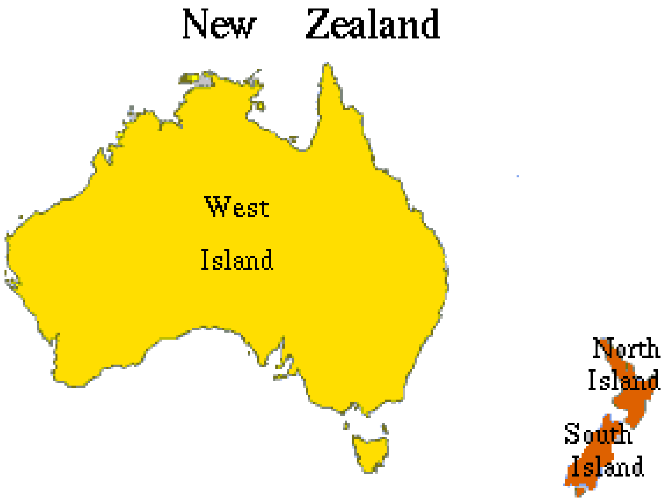
Steven Galbraith
and
Wenbo Mao

Mathematics Department,
Royal Holloway University of London
and
Hewlett-Packard Laboratories,
Bristol

steven.galbraith@rhul.ac.uk
wm@hplb.hpl.hp.com

http://www.isg.rhul.ac.uk/~sdg

A message from the New Zealand tourism board regarding ASIACRYPT 2002



Gennaro-Krawczyk-Rabin undeniable signatures

User has modulus N and $ed \equiv 1 \pmod{\varphi(N)}$. Let $g \in \mathbb{Z}_N^*$.

Public key: $(N, g, h = g^d)$.
Secret key: (d, e)

Undeniable signature on message m is

$$s = H(m)^d \pmod{N}.$$

Confirm (or deny) signature using ZK proofs that $(g, h, H(m), s)$ is (not) a Diffie-Hellman tuple in $\mathbb{Z}_N^*$.

Generalised from safe-prime products to general moduli by Galbraith, Mao and Paterson.

Anonymity

Given n users in a system and a single valid message-signature pair (m, s) can we guess who the signer is with probability non-negligibly better than $1/n$?

Attacks on anonymity

Suppose have n users with public moduli $N_1, \ldots, N_n$ and a valid message-signature pair (m, s).

- Know d odd, so $(\frac{H(m)}{N}) = (\frac{s}{N})$ for the valid signer.
  If $(\frac{H(m)}{N_i}) \neq (\frac{s}{N_i})$ then user i is not the signer.
- Know $1 \leq s < N$, so if $s > N_i$ for some i then know user i is not the signer.

More results

See the paper at
`http://www.isg.rhul.ac.uk/~sdg`
for details.

The following schemes do not provide anonymity:

- Chaum and van Antwerpen undeniable signature.
- Chaum confirmer scheme.
- Michels-Stadler.

Techniques in our paper allow anonymity:

- For a modified Chaum scheme even when users do not all work in the same finite field.
- For mixed systems, where users do not all use the same signature schemes.

New undeniable/confirmer scheme

System parameter for all users: A maximal bit length b for all moduli and signatures (e.g., $b = 2048$).

Preliminary signature on m is

$$s' = \xi H(m)^d \pmod{N}$$

where $\xi \in \mathbb{Z}_N^*$ is a randomly chosen square root of 1.

Final signature

$$s = s' + kN$$

where k is random such that $1 \leq s < 2^b$.

Send s as the signature.

Verification proceeds with a modular reduction and an extra squaring.