Threshold Cryptography with Asmuth-Bloom Secret Sharing

Kamer Kaya and Ali Aydın Selçuk

Department of Computer Engineering
Bilkent University

Asmuth-Bloom Secret Sharing Scheme

Secret Sharing:

1. Choose integers $m_0 < m_1 < \ldots < m_n$ s.t.
   - m_i are relatively prime
   - $m_0 > d$ is a prime
   - m_i satisfy (for perfectness)

$$\prod_{i=1}^{t} m_i \; > \; m_0 \prod_{i=1}^{t-1} m_{n-i+1}$$

2. Let $M = \prod_{i=1}^{t} m_i$. Compute

$$y = d + am_0$$

   where a is some random integer s.t. $0 \leq y < M$.

3. Share of the i^{th} user is

$$y_i = y \bmod m_i.$$

Sharing RSA with Asmuth-Bloom

Let $\mathcal{S}$ be a coalition of size t. Let $M_{\mathcal{S}} = \prod_{i\in\mathcal{S}} m_i$ and $M'_{\mathcal{S},i} = M^{-1}_{\mathcal{S}\setminus\{i\}} \pmod{m_i}$.

Secret construction is additive:

$$y = \sum_{i\in\mathcal{S}} y_i M'_{\mathcal{S},i} M_{\mathcal{S}\setminus\{i\}} \bmod M_{\mathcal{S}}$$
$$d = y \bmod m_0$$

hence may be suitable to share RSA:

$$w^d \bmod N = \prod_{i\in\mathcal{S}} w^{y_i\cdots} \bmod N$$

Challenge: But how to include (mod $M_{\mathcal{S}}$) in the exponent?

The Correction Procedure

- In the RSA signature setting with the public private key pair (e, d), the ith user contributes

$$s_i = w^{y_i M'_{\mathcal{S},i} M_{\mathcal{S}\setminus\{i\}} \bmod M_{\mathcal{S}}} \bmod N.$$

- The combiner computes the incomplete signature

$$\overline{s} = \prod_{i \in \mathcal{S}} s_i \bmod N.$$

  Then tries each $0 \leq j < t$ for

$$(\overline{s} w^{-j M_{\mathcal{S}}})^e \stackrel{?}{\equiv} w \pmod N$$

  and finds the j_0 satisfying the equality.

- The combiner computes the signature

$$s = \overline{s} w^{-j_0 M_{\mathcal{S}}} \pmod N$$

A FSS for RSA Signatures

1. RSA setup with $p = 2p' + 1$, $q = 2q' + 1$.
   $N = pq$; $ed \equiv 1 \pmod{\phi(N)}$.
   Use A-B to share d with a secret $m_0 = \phi(N) = 4p'q'$.

2. To sign w, user $i \in \mathcal{S}$ computes

$$u_i = y_i M'_{\mathcal{S},i} M_{\mathcal{S}\setminus\{i\}} \bmod M_{\mathcal{S}},$$
$$s_i = w^{u_i} \bmod N.$$

3. The *incomplete signature* $\overline{s}$ is

$$\overline{s} = \prod_{i \in \mathcal{S}} s_i \bmod N.$$

4. Let $\lambda = w^{-M_{\mathcal{S}}} \bmod N$ be the *corrector*. Try

$$(\overline{s}\lambda^j)^e = \overline{s}^e (\lambda^e)^j \stackrel{?}{\equiv} w \pmod{N} \qquad (1)$$

   for $0 \le j < t$. Then the signature s is

$$s = \overline{s}\lambda^\delta \bmod N$$

   where δ is the j value satisfying (1).

Extensions

- Provably secure threshold RSA, ElGamal and Paillier cryptosystems.

  K. Kaya, A. A. Selcuk, Threshold Cryptography Based on Asmuth-Bloom Secret Sharing, Information Sciences, 177 (19), pages 4148-4160, October 2007.

- Robust threshold RSA, ElGamal and Paillier cryptosystems.

  K. Kaya, A. A. Selcuk, Robust Threshold Schemes Based on the Chinese Remainder Theorem, Africacrypt 2008, Casablanca, Morocco, June 2008.

- Verifiability and proactivity for Asmuth-Bloom SSS. (In progress)