

Wednesday

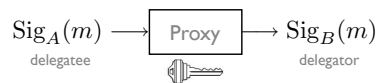
1

Sources

- “Divertible protocols and atomic proxy cryptography” by M. Blaze, G. Bleumer, and M. Strauss. EUROCRYPT '98.
- “Proxy Re-Signatures: New Definitions, Algorithms, and Applications” by Giuseppe Ateniese and Susan Hohenberger. ACM Computer and Communication Security (CCS), 2005.
- Thanks to Susan for providing most of the next slides.

2

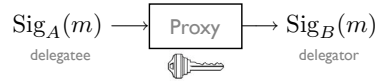
Proxy Re-signatures [BBS]



- Algs: KeyGen, Sign, Verify + ReKeyGen, ReSign
- * $\text{Key} = \text{ReKeyGen}(sk_A, sk_B)$
 $= \text{ReKeyGen}'(pk_A, sk_B)$
- * ReSign: Given key, proxy can change A's **valid** signature on m into B's **valid** signature on m .

3

Security



- Formal Security Definition
 - * strong unforge. against adapt. chosen-message attack [ADR02]
 - * malicious proxy cannot sign for A or B (only resign).
 - * malicious proxy and B cannot sign for A.
 - * malicious proxy and A get only "weak" secret key of B.

4

Proxy Re-Signatures vs. Proxy Signatures

[Blaze Bleumer Strauss 98]

[Mambo Usuda Okamoto 96,...]

$$\sigma_A(m) \rightarrow P \rightarrow \sigma_B(m)$$

$$\sigma_{B_1}(m) + \sigma_{B_2}(m) \rightarrow \sigma_B(m)$$

One SK for all delegations.

New SK for each delegation.

(Roughly) Proxy Re-Signatures are strict subset of Proxy Signatures.



Example: RSA-based Proxy Sigs.

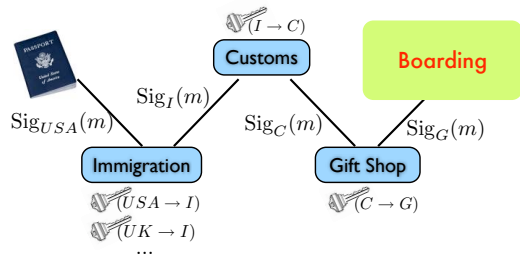
5

Our Contributions

- Formal security definition
- New applications
- Two secure constructions
 - * bidirectional scheme
 - * unidirectional scheme (with non-interactive delegation!)

6

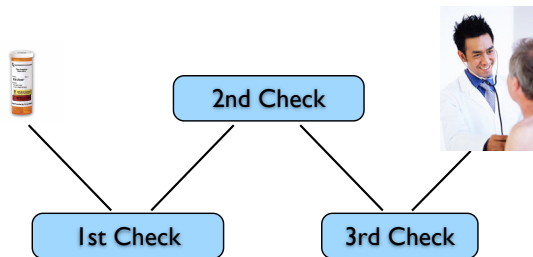
Proof of Path



Keep SK's offline. Hacker can't insert signatures in path by corrupting a node. Most nodes check only one sig against one PK.

7

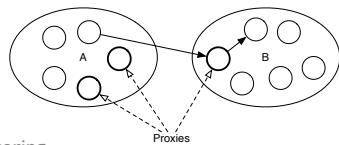
Proof of Flow



Can use cheap RFID tags and readers.

8

Other Applications



- certificate sharing
- (weak) group signatures
- signature delegation

9

Constructions

10

BBS Re-signatures

- * generator g
- * prime Q
- * hash H

$$PK = g^a$$

$$SK = a$$

Sign: (r, s) on m

$$r = g^k$$

$$s = aH(r, m) + k$$

$$\begin{matrix} \xrightarrow{(A \rightarrow B)} \\ \xleftarrow{(B \rightarrow A)} \end{matrix} = (b - a) \bmod Q$$

Bidirectional!

ReSign: $r' = r$

$$s' = s + \begin{matrix} \xrightarrow{(A \rightarrow B)} \\ \xleftarrow{(B \rightarrow A)} \end{matrix} H(r, m)$$

Problem: anyone can compute proxy key.

Worse Problem: Bob can compute Alice's secret key (and vice versa)!

11

Bilinear Maps to the Rescue



Let G_1, G_2 be cyclic groups of prime order q .

We say that a mapping $e : G_1 \times G_1 \rightarrow G_2$ is a **bilinear map** if it is:

1. Bilinear: $\forall g, h \in G_1, \forall a, b \in \mathbb{Z}_q, e(g^a, h^b) = e(g, h)^{ab}$
2. Non-degenerate: If g generates G_1 , then $e(g, g) \neq 1$.
3. Efficient: $\forall g, h \in G_1$, computing $e(g, h)$ is efficient.

12

Scheme One



[Based on Boneh-Lynn-Shacham'01 Signatures.]

* generator g $PK = g^a$
 * hash H $SK = a$

Sign: $s = H(m)^a$

$\left(\begin{smallmatrix} \leftarrow \\ (A \rightarrow B) \\ \leftarrow \\ (B \rightarrow A) \end{smallmatrix} \right) = (b/a)$
 Bidirectional!

ReSign: $s' = s \stackrel{(A \rightarrow B)}{\leftarrow} = H(m)^b$

Lots to like about this little scheme:
 short, efficient, secure, invisible, multi-use.

Secure under CDH in random oracle model.

13

Unidirectional Scheme?

Open problem since 1998.

14

Scheme Two



* generators g, h
 $PK = (g^a, h^{1/a})$
 $SK = a$ or h^a

Sign: (r, s) on m
 $s = aX$ (first-level) or
 $s = h^{aX}$ (second-level)

$\left(\begin{smallmatrix} \leftarrow \\ (A \rightarrow B) \end{smallmatrix} \right) = h^{b/a}$
 Unidirectional
 and non-interactive generation!

ReSign: $r' = r$
 $s' = \left(\begin{smallmatrix} \leftarrow \\ (A \rightarrow B) \end{smallmatrix} \right) \left(\begin{smallmatrix} aX \\ \leftarrow \\ h^{bX} \end{smallmatrix} \right) = h^{bX}$

Mostly solves open problem, but:
 (1) proxy key again public and (2) only single-use.

Secure under CDH and 2-DL in random oracle model.

15


<ul style="list-style-type: none"> * generators g, h * prime Q $PK = (g^a, h^{1/a})$ * hash H $SK = a$ * $e(g^a, g^b) = e(g, g)^{ab}$ 	Sign: (r, s) on m $r = g^k, t = a(H(r, m) + k)$ $s = t$ or h^t
$\left(\left(\frac{\cdot}{\cdot}\right)_{(A \rightarrow B)}\right) = h^{b/a}$ Non-interactive, Unidirectional: open problem since 1998.	ReSign: $r' = r$ $s' = \left(\left(\frac{t}{\cdot}\right)_{(A \rightarrow B)}\right) = h^{b(H(r, m) + k)}$

Pros: delegatee totally safe, unidirectional.
 Cons: public proxy key, single-use, non-invisible.

Secure under CDH and 2-DL in random oracle model.

16

Unidirectional Extensions




- Unidirectional + private proxy key: a scheme but no proof.
- Quick Revocation: broadcast one value at each time step to revoke all delegations.

17

Open Problems

- Unidirectional scheme with multi-use?
- Schemes without random oracles?
- Schemes without bilinear maps?
- Other applications?



18