A Multi-Use Unidirectional Proxy Re-Signature Scheme

A Signature for Artists?

T. Jonas Özgan

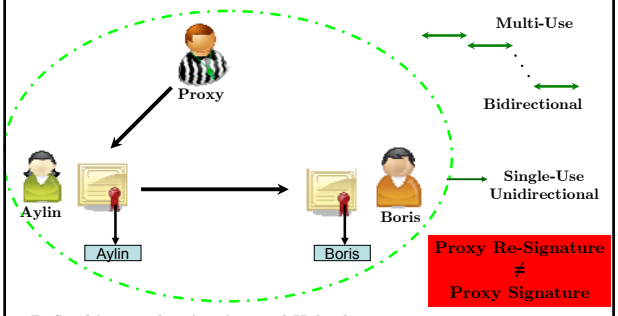
10 December 2009

A Brief History

- In 1998, Blaze, Bleumer and Strauss suggested Proxy Re-Signatures (as Atomic Proxy Cryptography)
- ... nothing
- Until 2005, Ateniese and Hohenberger: Proxy Re-Signatures: New Definitions, Algorithms, and Applications
  - Two Efficient Constructions, (Secure in the R.O.M)
    (1)Multi-Use Bidirectional
    (2)Single-Use Unidirectional
- ... and a left open challenge
- In 2008, Libert and Vergnaud: Multi-Use Unidirectional Proxy Re-Signatures

which we will analyse in detail....

What is a Proxy Re-Signature?



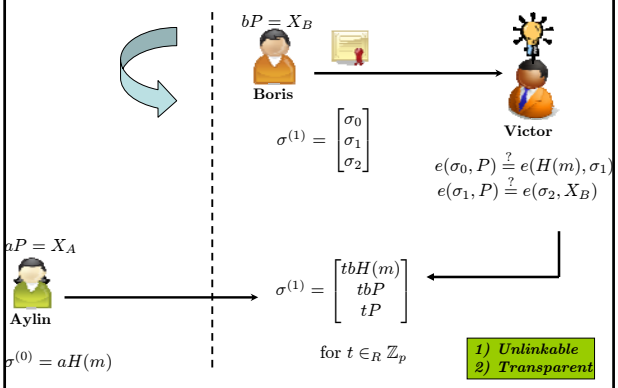
- Defined in 2005 by: Ateniese and Hohenberger.
  ... and the challenge was: Find a "*Multi-Use Unidirectional*" Scheme

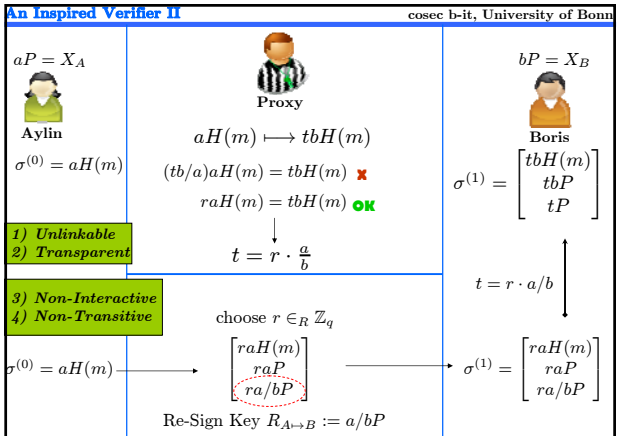
A Little Math...

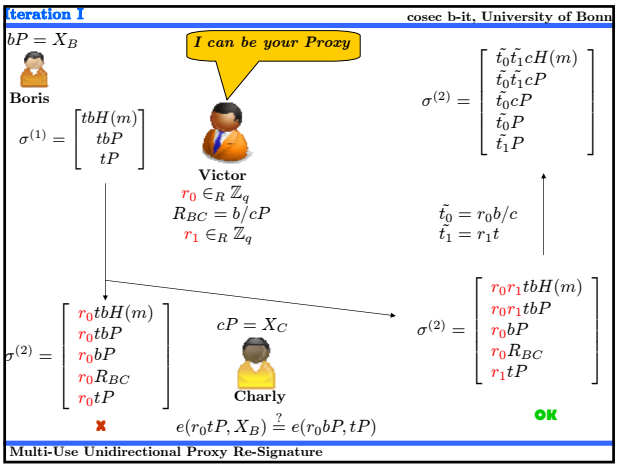
$\mathbb{G}$ and $\mathbb{G}_T$ commutative groups of prime order q,
(usually subgroups of an Elliptic Curve E)

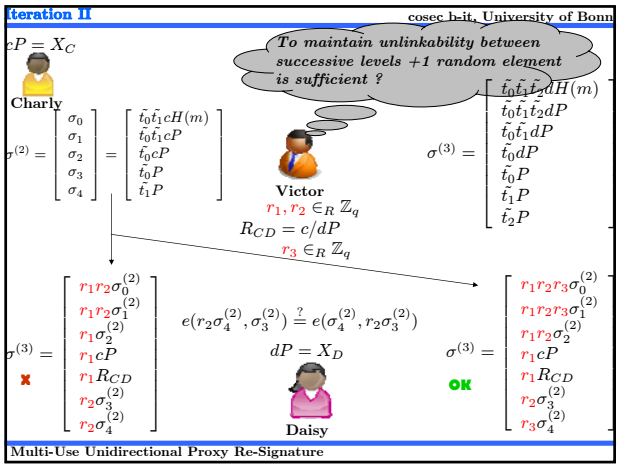
$e : \mathbb{G} \times \mathbb{G} \mapsto \mathbb{G}_T$ a mapping that is:

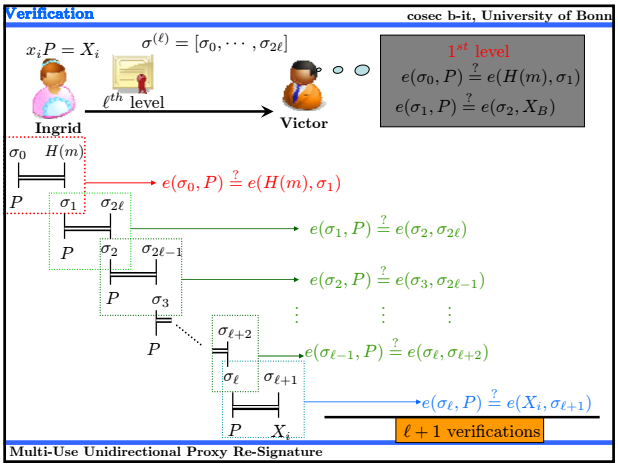
- bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, for any $P, Q \in \mathbb{G} \times \mathbb{G}$
- non-degenerate: $e(P, Q) \neq 1$, for some $P, Q \in \mathbb{G} \times \mathbb{G}$, with $P, Q \neq 1$
- $e(\cdot, \cdot)$ is efficiently computable for any input pair

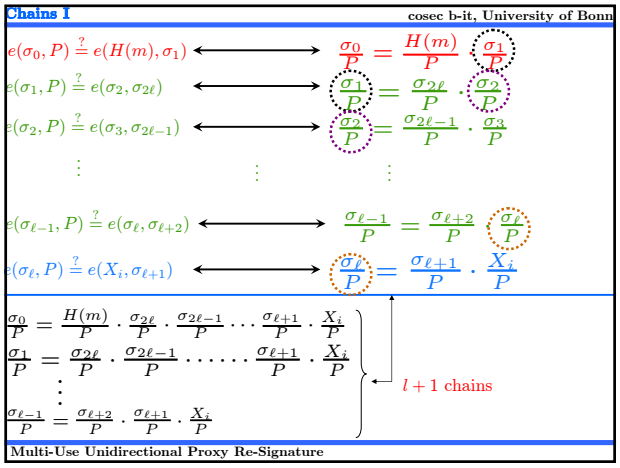


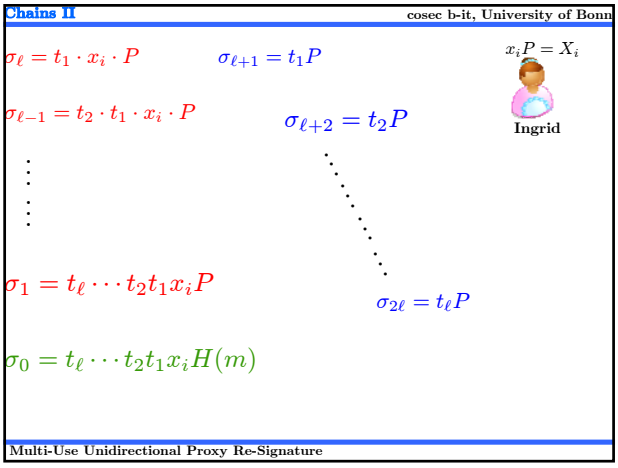


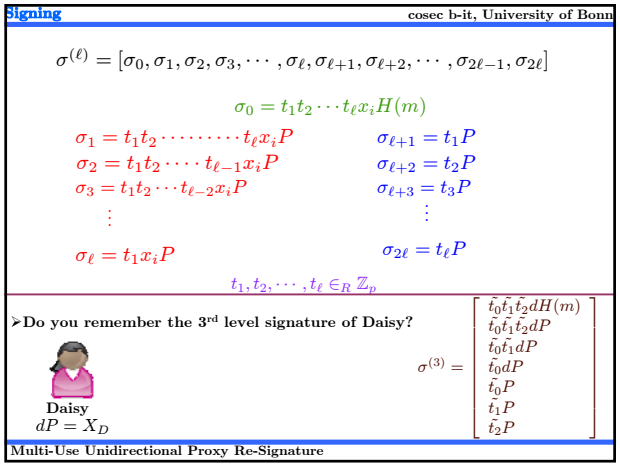

Iteration I
cosec b-it, University of Bonn
$bP = X_B$
Boris
$\sigma^{(1)} = \begin{bmatrix} tbH(m) \\ tbP \\ tP \end{bmatrix}$
I can be your Proxy
Victor
$r_0 \in_R \mathbb{Z}_q$
$R_{BC} = b/cP$
$r_1 \in_R \mathbb{Z}_q$
$\sigma^{(2)} = \begin{bmatrix} \tilde{t}_0\tilde{t}_1 cH(m) \\ \tilde{t}_0\tilde{t}_1 cP \\ \tilde{t}_0 cP \\ \tilde{t}_0 P \\ \tilde{t}_1 P \end{bmatrix}$
$\tilde{t}_0 = r_0 b/c$
$\tilde{t}_1 = r_1 t$
$\sigma^{(2)} = \begin{bmatrix} r_0 tbH(m) \\ r_0 tbP \\ r_0 bP \\ r_0 R_{BC} \\ r_0 tP \end{bmatrix}$
$cP = X_C$
Charly
$\sigma^{(2)} = \begin{bmatrix} r_0 r_1 tbH(m) \\ r_0 r_1 tbP \\ r_0 bP \\ r_0 R_{BC} \\ r_1 tP \end{bmatrix}$
OK
$e(r_0 tP, X_B) \stackrel{?}{=} e(r_0 bP, tP)$
Multi-Use Unidirectional Proxy Re-Signature


Iteration II
cosec b-it, University of Bonn
$cP = X_C$
Charly
$\sigma^{(2)} = \begin{bmatrix} \sigma_0 \\ \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \sigma_4 \end{bmatrix} = \begin{bmatrix} \tilde{t}_0\tilde{t}_1 cH(m) \\ \tilde{t}_0\tilde{t}_1 cP \\ \tilde{t}_0 cP \\ \tilde{t}_0 P \\ \tilde{t}_1 P \end{bmatrix}$
To maintain unlinkability between successive levels +1 random element is sufficient ?
Victor
$r_1, r_2 \in_R \mathbb{Z}_q$
$R_{CD} = c/dP$
$r_3 \in_R \mathbb{Z}_q$
$\sigma^{(3)} = \begin{bmatrix} \tilde{t}_0\tilde{t}_1\tilde{t}_2 dH(m) \\ \tilde{t}_0\tilde{t}_1\tilde{t}_2 dP \\ \tilde{t}_0\tilde{t}_1 dP \\ \tilde{t}_0 dP \\ \tilde{t}_0 P \\ \tilde{t}_1 P \\ \tilde{t}_2 P \end{bmatrix}$
$\sigma^{(3)} = \begin{bmatrix} r_1 r_2 \sigma_0^{(2)} \\ r_1 r_2 \sigma_1^{(2)} \\ r_1 \sigma_2^{(2)} \\ r_1 cP \\ r_1 R_{CD} \\ r_2 \sigma_3^{(2)} \\ r_2 \sigma_4^{(2)} \end{bmatrix}$
$e(r_2\sigma_4^{(2)}, \sigma_3^{(2)}) \stackrel{?}{=} e(\sigma_4^{(2)}, r_2\sigma_3^{(2)})$
$dP = X_D$
Daisy
$\sigma^{(3)} = \begin{bmatrix} r_1 r_2 r_3 \sigma_0^{(2)} \\ r_1 r_2 r_3 \sigma_1^{(2)} \\ r_1 r_2 \sigma_2^{(2)} \\ r_1 cP \\ r_1 R_{CD} \\ r_2 \sigma_3^{(2)} \\ r_3 \sigma_4^{(2)} \end{bmatrix}$
OK
Multi-Use Unidirectional Proxy Re-Signature


Verification
cosec b-it, University of Bonn
$x_i P = X_i$
Ingrid
$\sigma^{(\ell)} = [\sigma_0, \cdots, \sigma_{2\ell}]$
ℓ^{th} level
Victor
1^{st} level
$e(\sigma_0, P) \stackrel{?}{=} e(H(m), \sigma_1)$
$e(\sigma_1, P) \stackrel{?}{=} e(\sigma_2, X_B)$
$e(\sigma_0, P) \stackrel{?}{=} e(H(m), \sigma_1)$
$e(\sigma_1, P) \stackrel{?}{=} e(\sigma_2, \sigma_{2\ell})$
$e(\sigma_2, P) \stackrel{?}{=} e(\sigma_3, \sigma_{2\ell-1})$
$e(\sigma_{\ell-1}, P) \stackrel{?}{=} e(\sigma_\ell, \sigma_{\ell+2})$
$e(\sigma_\ell, P) \stackrel{?}{=} e(X_i, \sigma_{\ell+1})$
$\ell + 1$ verifications
Multi-Use Unidirectional Proxy Re-Signature


Chains I
cosec b-it, University of Bonn
$e(\sigma_0, P) \stackrel{?}{=} e(H(m), \sigma_1) \Leftrightarrow \frac{\sigma_0}{P} = \frac{H(m)}{P} \cdot \frac{\sigma_1}{P}$
$e(\sigma_1, P) \stackrel{?}{=} e(\sigma_2, \sigma_{2\ell}) \Leftrightarrow \frac{\sigma_1}{P} = \frac{\sigma_{2\ell}}{P} \cdot \frac{\sigma_2}{P}$
$e(\sigma_2, P) \stackrel{?}{=} e(\sigma_3, \sigma_{2\ell-1}) \Leftrightarrow \frac{\sigma_2}{P} = \frac{\sigma_{2\ell-1}}{P} \cdot \frac{\sigma_3}{P}$
$e(\sigma_{\ell-1}, P) \stackrel{?}{=} e(\sigma_\ell, \sigma_{\ell+2}) \Leftrightarrow \frac{\sigma_{\ell-1}}{P} = \frac{\sigma_{\ell+2}}{P} \cdot \frac{\sigma_\ell}{P}$
$e(\sigma_\ell, P) \stackrel{?}{=} e(X_i, \sigma_{\ell+1}) \Leftrightarrow \frac{\sigma_\ell}{P} = \frac{\sigma_{\ell+1}}{P} \cdot \frac{X_i}{P}$
$\frac{\sigma_0}{P} = \frac{H(m)}{P} \cdot \frac{\sigma_{2\ell}}{P} \cdot \frac{\sigma_{2\ell-1}}{P} \cdots \frac{\sigma_{\ell+1}}{P} \cdot \frac{X_i}{P}$
$\frac{\sigma_1}{P} = \frac{\sigma_{2\ell}}{P} \cdot \frac{\sigma_{2\ell-1}}{P} \cdot \cdots \cdot \frac{\sigma_{\ell+1}}{P} \cdot \frac{X_i}{P}$
$\frac{\sigma_{\ell-1}}{P} = \frac{\sigma_{\ell+2}}{P} \cdot \frac{\sigma_{\ell+1}}{P} \cdot \frac{X_i}{P}$
$l + 1$ chains
Multi-Use Unidirectional Proxy Re-Signature


Chains II
cosec b-it, University of Bonn
$\sigma_\ell = t_1 \cdot x_i \cdot P$
$\sigma_{\ell+1} = t_1 P$
$x_i P = X_i$
Ingrid
$\sigma_{\ell-1} = t_2 \cdot t_1 \cdot x_i \cdot P$
$\sigma_{\ell+2} = t_2 P$
$\sigma_1 = t_\ell \cdots t_2 t_1 x_i P$
$\sigma_{2\ell} = t_\ell P$
$\sigma_0 = t_\ell \cdots t_2 t_1 x_i H(m)$
Multi-Use Unidirectional Proxy Re-Signature


Signing
cosec b-it, University of Bonn
$\sigma^{(\ell)} = [\sigma_0, \sigma_1, \sigma_2, \sigma_3, \cdots, \sigma_\ell, \sigma_{\ell+1}, \sigma_{\ell+2}, \cdots, \sigma_{2\ell-1}, \sigma_{2\ell}]$
$\sigma_0 = t_1 t_2 \cdots t_\ell x_i H(m)$
$\sigma_1 = t_1 t_2 \cdots \cdots t_\ell x_i P$
$\sigma_2 = t_1 t_2 \cdots t_{\ell-1} x_i P$
$\sigma_3 = t_1 t_2 \cdots t_{\ell-2} x_i P$
$\sigma_\ell = t_1 x_i P$
$\sigma_{\ell+1} = t_1 P$
$\sigma_{\ell+2} = t_2 P$
$\sigma_{\ell+3} = t_3 P$
$\sigma_{2\ell} = t_\ell P$
$t_1, t_2, \cdots, t_\ell \in_R \mathbb{Z}_p$
➢Do you remember the 3rd level signature of Daisy?
Daisy
$dP = X_D$
$\sigma^{(3)} = \begin{bmatrix} \tilde{t}_0\tilde{t}_1\tilde{t}_2 dH(m) \\ \tilde{t}_0\tilde{t}_1\tilde{t}_2 dP \\ \tilde{t}_0\tilde{t}_1 dP \\ \tilde{t}_0 dP \\ \tilde{t}_0 P \\ \tilde{t}_1 P \\ \tilde{t}_2 P \end{bmatrix}$
Multi-Use Unidirectional Proxy Re-Signature

Re-Signing

Ingrid

$x_i P = X_i$

$\sigma^{(\ell)} = [\sigma_0, \sigma_1, \sigma_2, \sigma_3, \cdots, \sigma_\ell, \sigma_{\ell+1}, \sigma_{\ell+2}, \cdots, \sigma_{2\ell-1}, \sigma_{2\ell}]$

Proxy

$R_m = x_i / x_m P$

$r_0, r_1, \cdots, r_\ell \in_R \mathbb{Z}_p$

$r_0 r_1 \cdots\cdots\cdots r_\ell \; \sigma_0$

$r_0 r_1 \cdots\cdots\cdots r_\ell \; \sigma_1$

$r_0 r_1 \cdots\cdots r_{\ell-1} \; \sigma_2$

$r_0 r_1 \cdots r_{\ell-2} \; \sigma_3$

$r_0 r_1 \; \sigma_\ell$

$r_0 \; X_i$

$r_0 \; R_m$

$r_1 \; \sigma_{\ell+1}$

$r_2 \; \sigma_{\ell+2}$

$r_3 \; \sigma_{\ell+3}$

$r_\ell \; \sigma_{2\ell}$

$x_m P = X_m$

Mandy

$\sigma^{(\ell+1)} = [\sigma_0, \sigma_1, \cdots, \sigma_{2\ell+2}]$

Open Questions

➢Are *l* coefficients necessary for generating an *l-th* level signature ?

Yes!

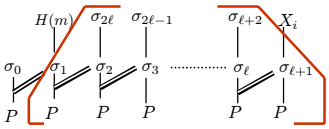
✓Using less destroys the unlinkability

✓Using same coefficient twice also

➢Can we make the Signature Shorter ?

Possibly not

The Chain Shortening Problem [CSP]



Security I

➢We always make some assumptions, to say: *"It is Secure"*

$aP = X_A$

Aylin

$\sigma^{(0)} = aH(m)$

Secure under the Computational Diffie-Hellman [CDH] assumption...

Given:

$[\, P, X_A, H(m') = h'P \,]$ **find** $ah'P = aH(m')$

HARD!

$x_m P = X_m$

$\sigma^{(\ell+1)} = [\sigma_0, \cdots, \sigma_{2\ell+2}]$

We need to introduce other assumptions:

•Computational Diffie-Hellman [CDH]

➢Modified CDH [mCDH]

➢2-out-of-3-Diffie-Hellman [2-3-CDH]

L-Flexible-Diffie-Hellman [L-Flex-DH]

Security II

CDH:

Given:

[P, aP, bP] **find** ***abP***

mCDH:

Given:

[P, aP, a^{-1}P, bP] **find** ***abP***

2-3-CDH:

Given:

[P, aP, bP] **find** [Q, abQ]

1-Flex-CDH:

Given:

[P, aP, bP] **find** [Q, aQ, abQ]

2-Flex-CDH:

$$\left[\begin{pmatrix} m_1 P, & m_2 P, \\ am_1 P, & am_1 m_2 P, \end{pmatrix}, abm_1 m_2 P\right]$$

L-Flex-CDH:

Given:

[P, aP, bP] **find** $\left[\begin{pmatrix} t_1 P & , \cdots , & t_\ell P, \\ at_1 P, at_1 t_2 P & , \cdots , & at_1 \cdots t_\ell P, \end{pmatrix}, abt_1 \cdots t_\ell P\right]$

Security III

➢The View of Security

Proxy

Aylin

Boris

Internal Security

Eric

4. External Security

➢*Can Eric forge a signature?*

1. Limited Proxy Security

➢*Can the Proxy Sign Messages for Aylin or Boris ?*

2. Delegatee Security

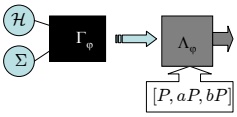
➢*Is Boris protected if Aylin also impersonates Proxy ?*

3. Delegator Security

➢*Is Aylin protected if Boris also impersonates Proxy ?*

Security IV

Limited Proxy Security Delegatee Security External Security



$$\left[\begin{pmatrix} t_1 P & , \cdots , & t_\ell P, \\ at_1 P & , \cdots , & at_1 \cdots t_\ell P, \end{pmatrix}, abt_1 \cdots t_\ell P\right]$$

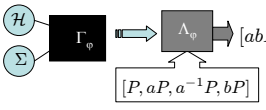
▪Successful evil Proxy Γ_1 implies algorithm Λ_1 which solves the *L-Flex-DH*

▪Successful evil Aylin Γ_2 implies algorithm Λ_2 which solves the *L-Flex-DH*

▪Successful evil Eric Γ_4 implies algorithm Λ_4 which solves the *L-Flex-DH*

▪Successful evil Boris Γ_3 implies Algorithm Λ_3 which solves the *mCDH*

Delegator Security



There is a way to eliminate the Random Oracle(s) ... i.e. The Signature Scheme is also secure in the standard model

THANK YOU

Questions?

cosec b-it, University of Bonn

Multi-Use Unidirectional Proxy Re-Signature

cosec b-it, University of Bonn

$$\left[\begin{pmatrix} t_1 P, & \cdots, & t_\ell P, \\ at_1 P, & \cdots, & at_1 \cdots t_\ell P, \end{pmatrix}, abt_1 \cdots t_\ell P\right]$$

Set $t_0 = r_0 x_i / x_j$ and $t_k = r_k t_k$ for $k \in [1, \ell]$

Multi-Use Unidirectional Proxy Re-Signature