Two Secure Anonymous Proxy-based Data Storages *

Olivier Blazy[1] **Xavier Bultel**[2] Pascal Lafourcade[2]

Université de Limoges, Xlim, Limoges, France

Clermont Université Auvergne, LIMOS, Clermont-Ferrand, France

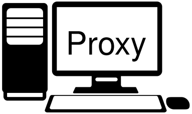
July 29, 2016

SECRYPT 2016, Lisbon

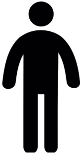
*This research was conducted with the support of the “Digital Trust” Chair from the University of Auvergne Foundation.

Proxy Re-Encryption (PRE)

Alice $(\mathrm{pk}_a, \mathrm{sk}_a)$

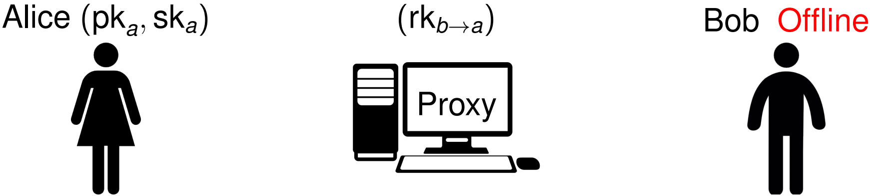


Bob $(\mathrm{pk}_b, \mathrm{sk}_b)$

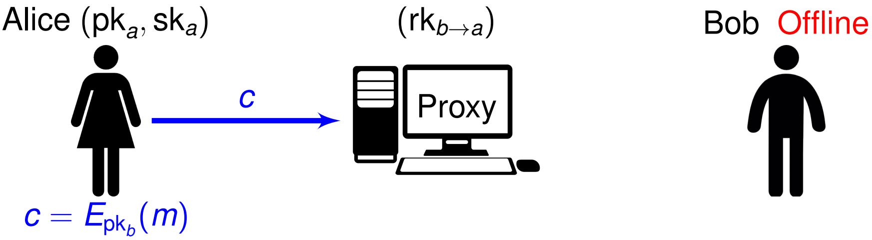


Proxy Re-Encryption (PRE)

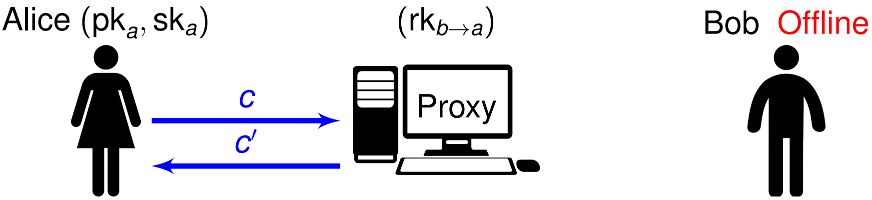
Proxy Re-Encryption (PRE)



Proxy Re-Encryption (PRE)



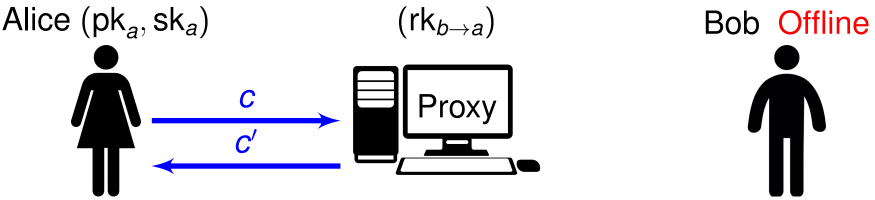
Proxy Re-Encryption (PRE)



$$c = E_{\mathrm{pk}_b}(m)$$

$$c' = RE_{\mathrm{rk}_{b \to a}}(c) = E_{\mathrm{pk}_a}(m)$$

Proxy Re-Encryption (PRE)

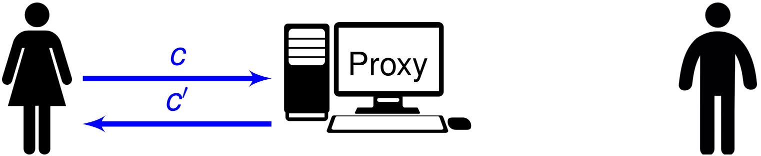


$$c = E_{\mathsf{pk}_b}(m)$$
$$m = D_{\mathsf{sk}_a}(c')$$

$$c' = RE_{\mathsf{rk}_{b\to a}}(c)$$
$$= E_{\mathsf{pk}_a}(m)$$

Proxy Re-Encryption (PRE)

Alice $(\mathrm{pk}_a, \mathrm{sk}_a)$ $(\mathrm{rk}_{b\to a})$ Bob Offline



$c = E_{\mathrm{pk}_b}(m)$

$m = D_{\mathrm{sk}_a}(c')$

$c' = RE_{\mathrm{rk}_{b\to a}}(c)$

$= E_{\mathrm{pk}_a}(m)$

P learns nothing about *m* (IND-CPA).

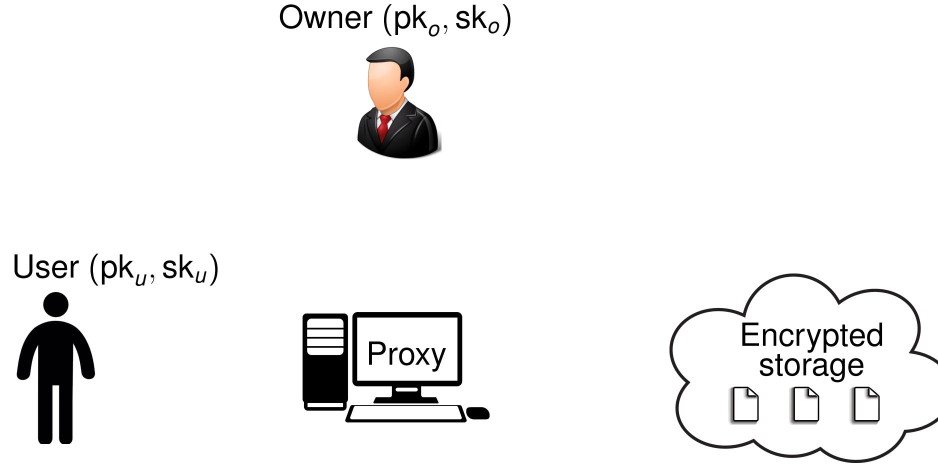
PRE History

- Blaze *et al.* (1998) First definition of PRE.
- Ivan *et al.* (2003) Formal treatment.
- Ateniese *et al.* (2006) Unidirectional PRE.
- Canetti *et al.* (2007) CCA security.
- Libert *et al.* (2007) Unidirectional + CCA.

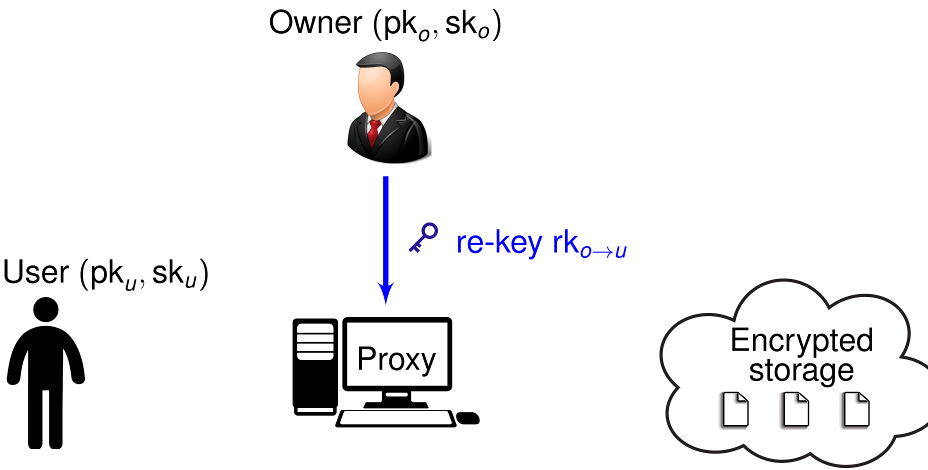
PRE History

- Blaze *et al.* (1998) First definition of PRE.
- Ivan *et al.* (2003) Formal treatment.
- Ateniese *et al.* (2006) Unidirectional PRE.
  New application: encrypted storage management.
- Canetti *et al.* (2007) CCA security.
- Libert *et al.* (2007) Unidirectional + CCA.

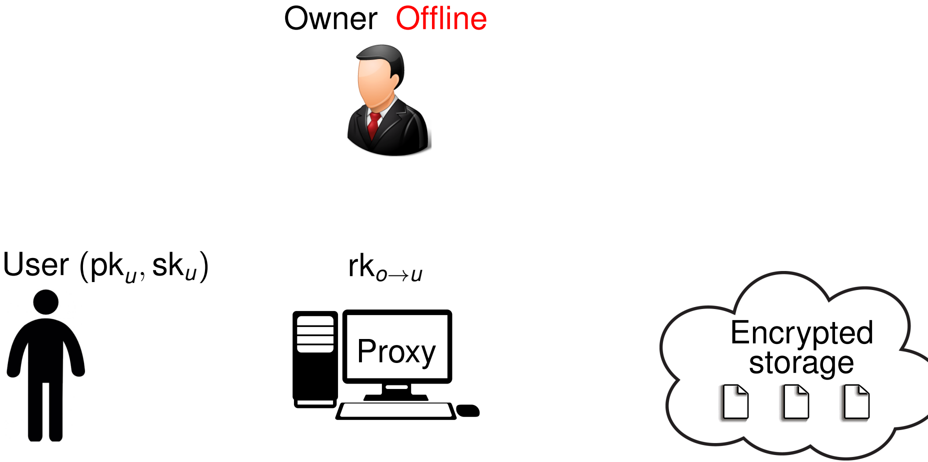
PRE based storage



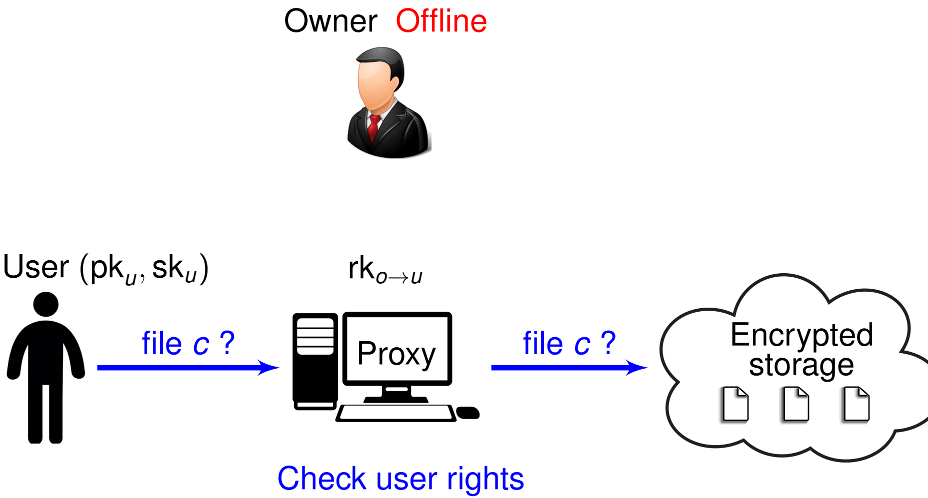
PRE based storage



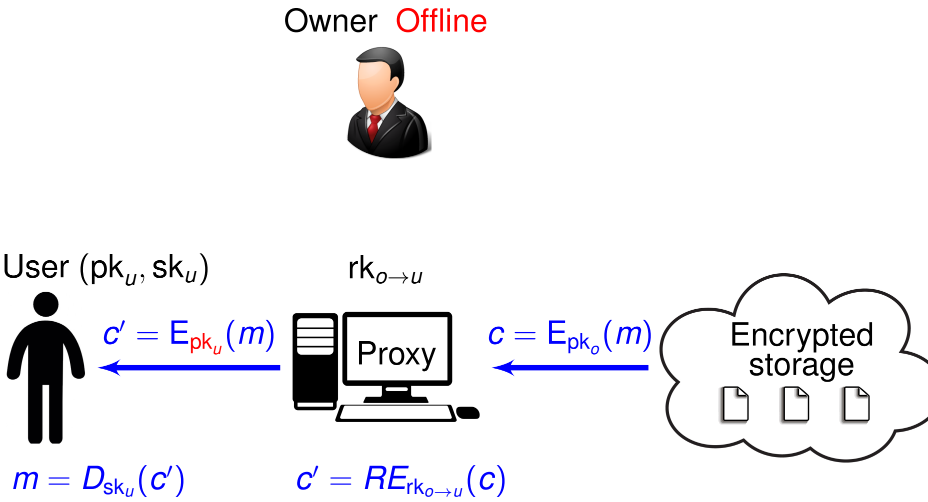
PRE based storage



PRE based storage



PRE based storage

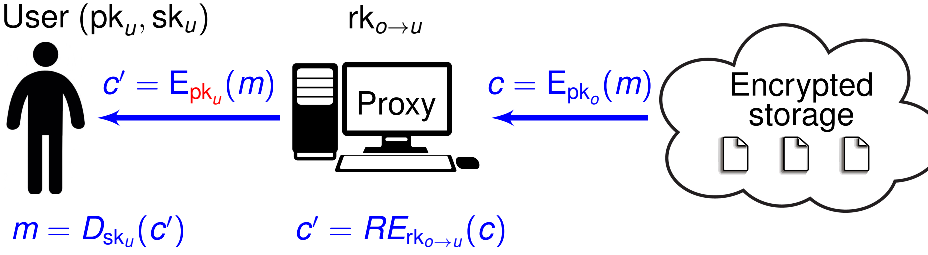


PRE based storage

Owner Offline

Semi-trust proxy:

- No info about m
- P knows U id.
- P knows U rights
- P knows c



PRE based storage

Semi-trust proxy:

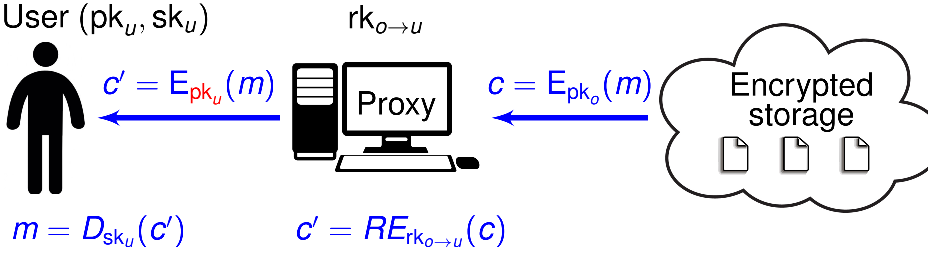
-No info about m

-P knows U id.

-P knows U rights

-P knows c

Goal: more privacy!



PRE & anonymity?

- Ateniese *et al.* (2009) Anonymous re-encryption key.
- Shao *et al.* (2012) Anonymity for recipient message.
- Zheng *et al.* (2014) Anonymous re-encryption key + CCA.

PRE & anonymity?

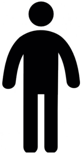
- Ateniese *et al.* (2009) Anonymous re-encryption key.
- Shao *et al.* (2012) Anonymity for recipient message.
- Zheng *et al.* (2014) Anonymous re-encryption key + CCA.

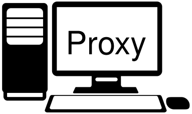
$\rightarrow$ Only partial anonymity.

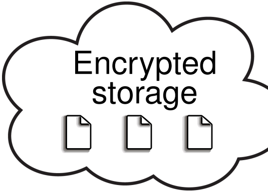
Our idea

Owner (pkg_i, skg_i)

User

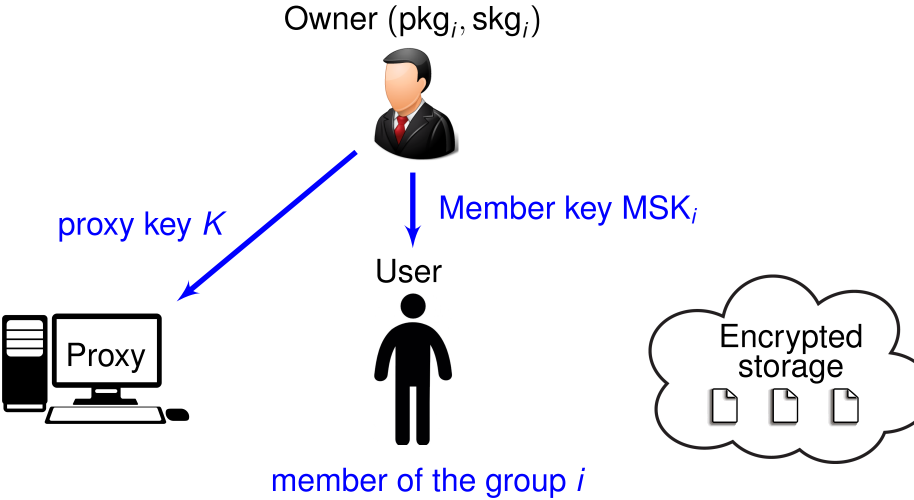




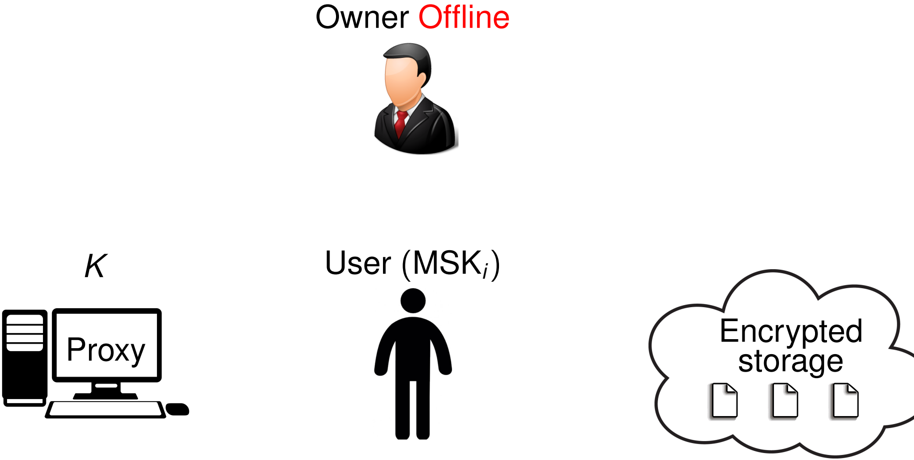


member of the group i

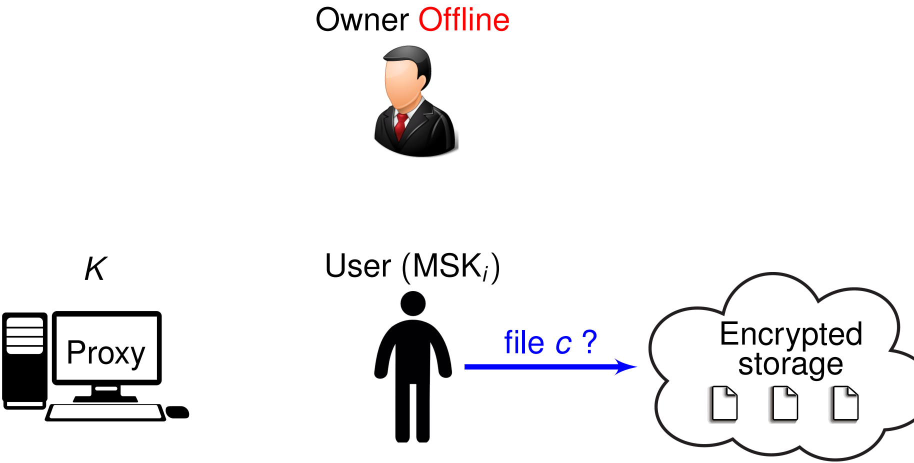
Our idea


Owner ($\mathsf{pkg}_i, \mathsf{skg}_i$)
proxy key K
Member key MSK_i
User
Proxy
Encrypted storage
member of the group i

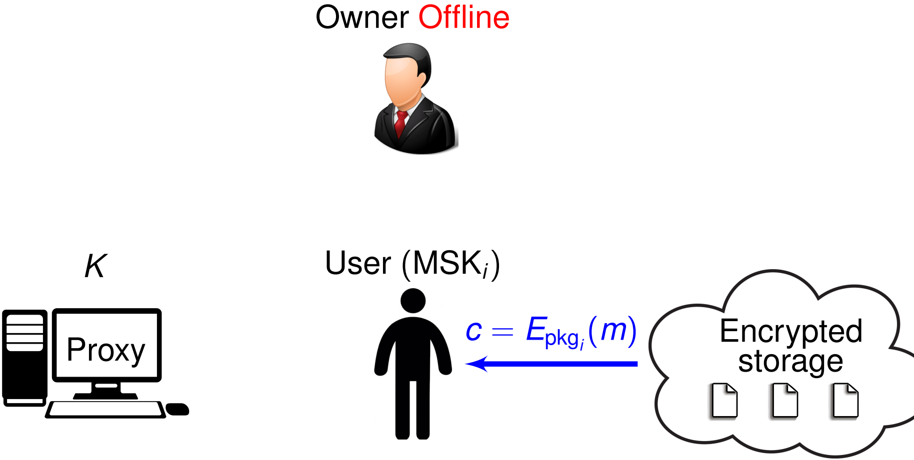
Our idea



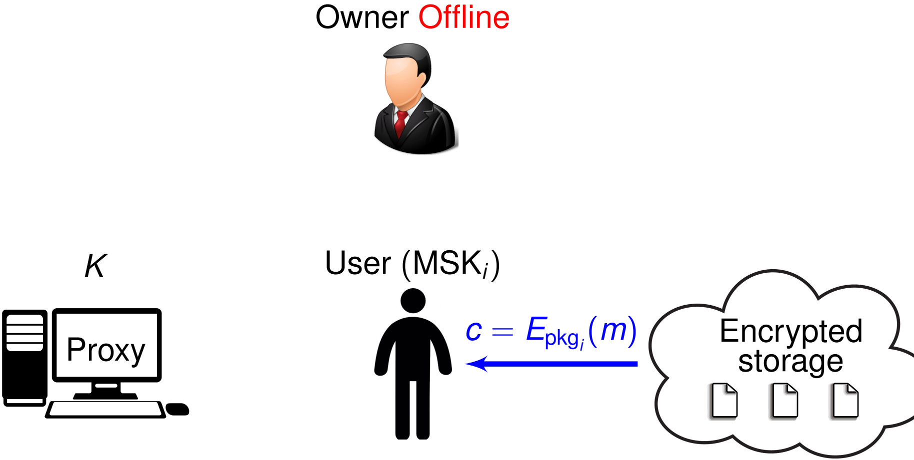
Our idea



Our idea



Our idea

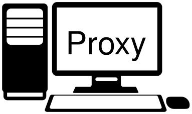


User knows
MSK$_i$ and c

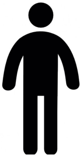
Our idea

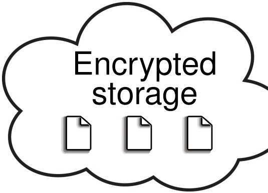
Owner Offline

K



User (MSK_i)

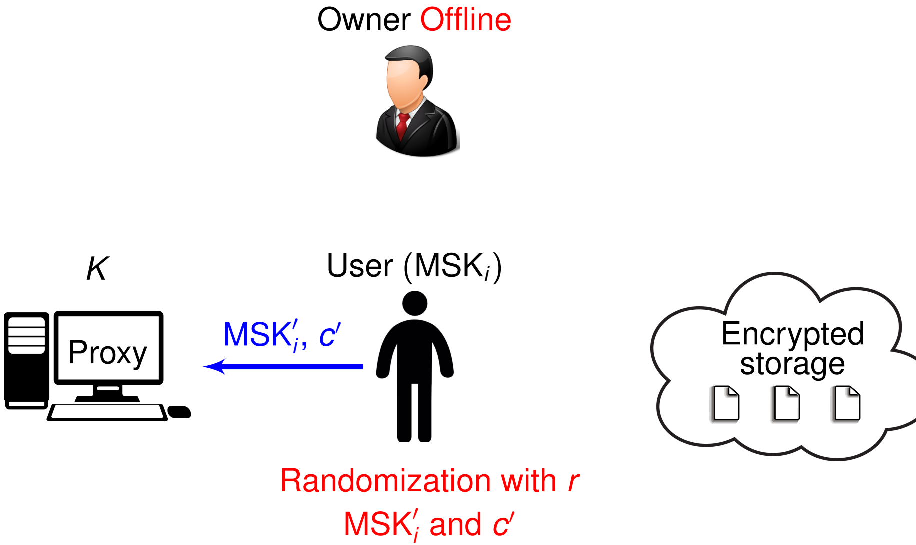




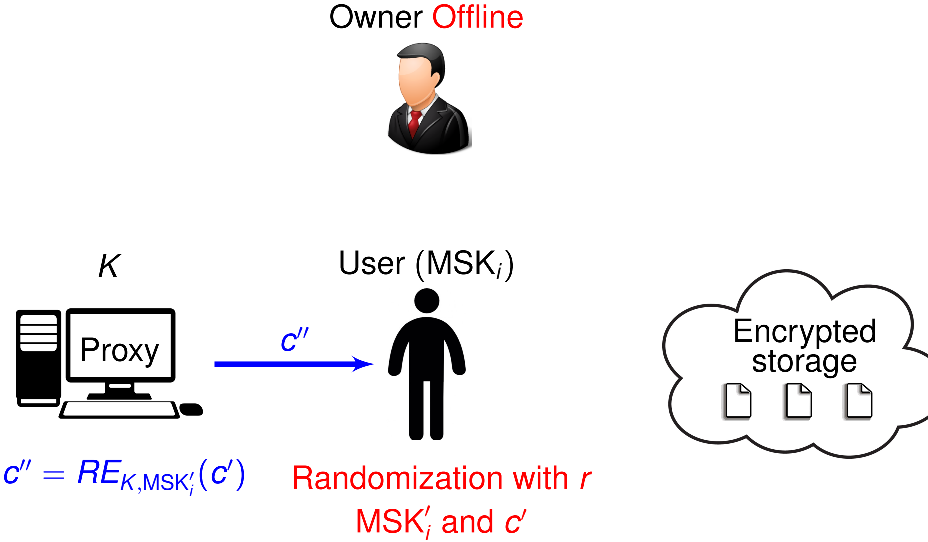
Randomization with r

MSK'_i and c'

Our idea

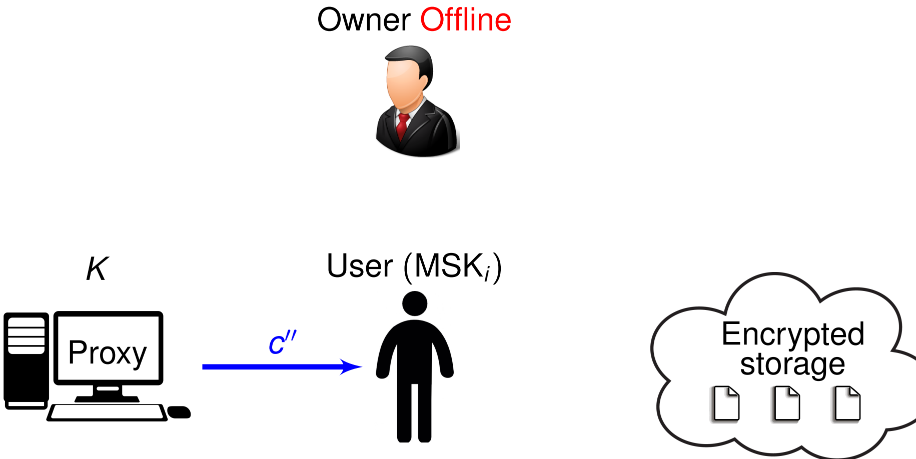

Owner Offline
K
User (MSK_i)
Proxy
MSK'_i, c'
Encrypted storage
Randomization with r
MSK'_i and c'

Our idea



Owner Offline
K
Proxy
c''
User (MSK_i)
Encrypted storage
$c'' = RE_{K,MSK_i'}(c')$
Randomization with r
MSK_i' and c'

Our idea



$c'' = RE_{K,\mathrm{MSK}'_i}(c')$

$m = D_r(c'')$

Our idea

Semi-trust proxy:

-No info about m

-No info about U id.

-No info about i

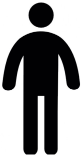
-No info about c

Owner Offline

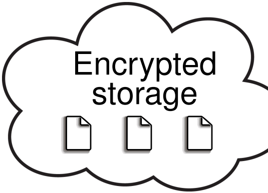
K

MSK'_i and c'

User (MSK_i)



$m = D_r(c'')$



Our contribution

Two schemes:

Our contribution

Two schemes:

DRAS: **Direct revocation mechanism**: The owner can revoke anybody anytime.

- Pay-per-download model.
- Weak anonymity.

Our contribution

Two schemes:

DRAS: **Direct revocation mechanism**: The owner can revoke anybody anytime.

- Pay-per-download model.
- Weak anonymity.

IRAS: **Indirect revocation mechanism**: the owner can revoke users periodically.

- Monthly-fee model.
- Full anonymity.

DRAS

P-Gen($\mathcal{P}$): generate proxy keys $(\mathsf{PKP}, \mathsf{SKP})$.

G-Gen($\mathcal{P}$): generate group key $(\mathsf{PKG}_j, \mathsf{SKG}_j)$.

Join($\mathsf{SKG}_j, \mathsf{WL}, U_i$): generate a group member key MSK_i^j.

Encrypt(PKG_j, m): encrypt m for group j.

Revoke($\mathsf{MSK}_i^j, \mathsf{BL}$): revoke a user.

Open($\mathsf{VIEW}, \mathsf{WL}$): desanonymize a transaction.

ProxyDec(U_i, P): decryption protocol between a user and the proxy.

DRAS

Keys construction:

- Proxy keys $(\mathsf{PKP}, \mathsf{SKP})$ for an encryption scheme.
- Group key $(\mathsf{PKG}, \mathsf{SKG}) = (g^\gamma, \gamma)$.
- Member key $\mathsf{MSK} = (t, \mathsf{Enc}_{\mathsf{PKP}}(\frac{t}{\gamma}))$.

DRAS

Keys construction:

- Proxy keys $(\mathsf{PKP}, \mathsf{SKP})$ for an encryption scheme.
- Group key $(\mathsf{PKG}, \mathsf{SKG}) = (g^\gamma, \gamma)$.
- Member key $\mathsf{MSK} = (t, \mathsf{Enc}_{\mathsf{PKP}}(\frac{t}{\gamma}))$.

The encryption algorithm is an ElGamal variant:

Keys Secret $\mathsf{sk} = x$, public $\mathsf{pk} = g^x$.

Encryption Pick r and compute $(C_1, C_2) = (\mathsf{pk}^r, g^r \cdot m)$.

Decryption Compute $m = \frac{C_2}{C_1^{1/\mathsf{sk}}}$

DRAS: Decryption protocol

- $C = (C_1, C_2) = (g^{r \cdot \gamma}, g^r \cdot m)$
- $\mathsf{MSK} = (\mathsf{MSK}_1, \mathsf{MSK}_2) = (t, \mathsf{Enc}_{\mathsf{PKP}}(\frac{t}{\gamma}))$

DRAS: Decryption protocol

- $C = (C_1, C_2) = (g^{r\cdot\gamma}, g^r \cdot m)$
- $\mathsf{MSK} = (\mathsf{MSK}_1, \mathsf{MSK}_2) = (t, \mathsf{Enc}_{\mathsf{PKP}}(\frac{t}{\gamma}))$

(PKP; MSK; C)		(SKP; BL)
$s \xleftarrow{\$} \mathbb{Z}_p^*$; $B = (C_1)^s$	$\xrightarrow{B,\mathsf{MSK}_2}$	If $\mathsf{MSK}_2 \in \mathsf{BL}$ then abort;
		else $w = \mathsf{Dec}_{\mathsf{SKP}}(\mathsf{MSK}_2)$
$m = \frac{C_2}{D^{(1/s\cdot t)}}$	$\xleftarrow{D}$	$D = (B)^w = (C_1^s)^{\frac{t}{\gamma}} = g^{s\cdot r\cdot t}$
$= \frac{g^r\cdot m}{g^{s\cdot r\cdot t\cdot\frac{1}{s\cdot t}}} = \frac{g^r\cdot m}{g^r}$		
Output m		Output $\mathsf{VIEW} = \mathsf{MSK}_2$.

DRAS: Decryption protocol

- $C = (C_1, C_2) = (g^{r\cdot\gamma}, g^r \cdot m)$
- $\mathsf{MSK} = (\mathsf{MSK}_1, \mathsf{MSK}_2) = (t, \mathsf{Enc}_{\mathsf{PKP}}(\frac{t}{\gamma}))$

(PKP; MSK; C) (SKP; BL)

$s \xleftarrow{\$} \mathbb{Z}_p^*$; $B = (C_1)^s$ $\xrightarrow{B,\mathsf{MSK}_2\mathsf{MSK}_2}$ If $\mathsf{MSK}_2 \in \mathsf{BL}$ then abort;

else $w = \mathsf{Dec}_{\mathsf{SKP}}(\mathsf{MSK}_2) = \frac{t}{\gamma}$

$m = \frac{C_2}{D^{(1/s\cdot t)}}$ $\xleftarrow{D}$ $D = (B)^w = (C_1^s)^{\frac{t}{\gamma}} = g^{s\cdot r\cdot t}$

$= \frac{g^r \cdot m}{g^{s\cdot r\cdot t\cdot \frac{1}{s\cdot t}}} = \frac{g^r\cdot m}{g^r}$

Output m Output $\mathsf{VIEW} = \mathsf{MSK}_2$.

Proxy links user who uses two times the same member key

ElGamal is malleable

- $C = (g^r, g^{x \cdot r}.m)$
- $C' = ((g^r)^s, (g^{x \cdot r}.m)^s) = (g^{(r \cdot s)}, g^{(r \cdot s) \cdot x} \cdot m^s)$.
- Decryption: $m' = m^s = \frac{g^{(r \cdot s) \cdot x} \cdot (m^s)}{g^{(r \cdot s)}}$.
- Difficult to link C and C' (Diffie-Hellman problem).
- The message m is hidden.

Indirect Revocation Anonymous Storage

O-Gen($\mathcal{P}$): generate owner $(\mathsf{PKO}, \mathsf{SKO})$.

P-Gen($\mathcal{P}$): generate proxy key pair $(\mathsf{PKP}, \mathsf{SKP})$.

G-Gen($\mathcal{P}$): generate group key pair $(\mathsf{PKG}, \mathsf{SKG})$.

Join($\mathsf{SKG}_j, \mathsf{SKO}, \mathsf{PKP}$): generate a group member key MSK.

O-Update($\mathsf{SKO}, \mathsf{PKO}$): update $(\mathsf{PKO}, \mathsf{SKO})$.

U-Update($\mathsf{MSK}_i^j, \mathsf{SKO}$): update MSK.

Encrypt(PKG_j, m): encrypt a message m.

ProxyDec(U_i, P): decryption protocol between a user and the proxy.

(Simplified) IRAS parameters

Keys constructions:

- $\mathcal{P} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, \mathsf{PKE}, \mathcal{S})$.
- Proxy keys $(\mathsf{PKP}, \mathsf{SKP}) = (g_2^p, p)$.
- Group keys $(\mathsf{PKG}, \mathsf{SKG}) = (g_1^\gamma, \gamma)$.
- Member key $\mathsf{MSK} = (g_2^{p \cdot s}, g_2^s \cdot g_2^{1/\gamma})$.

(Simplified) IRAS parameters

Keys constructions:

- $\mathcal{P} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, \mathsf{PKE}, \mathcal{S})$.
- Proxy keys $(\mathsf{PKP}, \mathsf{SKP}) = (g_2^p, p)$.
- Group keys $(\mathsf{PKG}, \mathsf{SKG}) = (g_1^\gamma, \gamma)$.
- Member key $\mathsf{MSK} = (g_2^{p \cdot s}, g_2^s \cdot g_2^{1/\gamma})$.

The encryption algorithm is an ElGamal bilinear variant:

Keys Secret $\mathsf{sk} = x$, public $\mathsf{pk} = g_1^x$.

Encryption Pick r and compute $(C_1, C_2) = (\mathsf{pk}^r, e(g_1, g_2)^r \cdot m)$.

Decryption Compute $m = \frac{C_2}{e(C_1, g_2)^{1/\mathsf{sk}}}$

(Simplified) Decryption protocol

- $C = (C_1, C_2) = (g_1^{r\cdot\gamma}, e(g_1, g_2)^r \cdot m)$
- $\mathrm{MSK} = (\mathrm{MSK}_1, \mathrm{MSK}_2) = (g_2^{p\cdot s}, g_2^s \cdot g_2^{\frac{1}{\gamma}})$

(Simplified) Decryption protocol

- $C = (C_1, C_2) = (g_1^{r\cdot\gamma}, e(g_1, g_2)^r \cdot m)$
- $\mathsf{MSK} = (\mathsf{MSK}_1, \mathsf{MSK}_2) = (g_2^{p\cdot s}, g_2^s \cdot g_2^{\frac{1}{\gamma}})$

$(C; \mathsf{MSK})$ (p)

$\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p^*$

$\mathsf{MSK}' = (\mathsf{MSK}_1^\alpha, \mathsf{MSK}_2^\alpha)$

$C_1' = C_1^\beta$ $\xrightarrow{C_1', \mathsf{MSK}'}$ $D = e(g_1^{r\cdot\gamma\cdot\beta}, \frac{\mathsf{MSK}_2'}{\mathsf{MSK'}_1^{1/p}})$

$m = \frac{C_2}{D^{\frac{1}{\alpha\cdot\beta}}} = \frac{e(g_1,g_2)^r\cdot m}{e(g_1,g_2)^{\frac{r\cdot\alpha\cdot\beta}{\alpha\cdot\beta}}}$ $\xleftarrow{D}$ $= e(g_1, g_2)^{r\cdot\alpha\cdot\beta}$

Provable IRAS

Many tools to construct a provable scheme:

- Proof of a signature on MSK from MSK′.
- Revocation: The owner updates his signing key, but does not re-sign MSK.
- Damgård-ElGamal (CCA1).
- Smooth projective hash functions.

DRAS

- Direct revocation.
- Simple and efficient scheme.
- CPA secure.
- Not fully anonymous.

IRAS

- Indirect revocation.
- Not efficient, use complex tools to be provably secure.
- CPA secure.
- Fully anonymous.

Future work

- Increase and simplify IRAS.
- Without Damgård-ElGamal and SPHF.

Thank you for your attention.

Questions?