

An Efficient Anonymous Credential System

Norio Akagi (Kyoto University)

Yoshifumi Manabe (Kyoto University, NTT Laboratories)

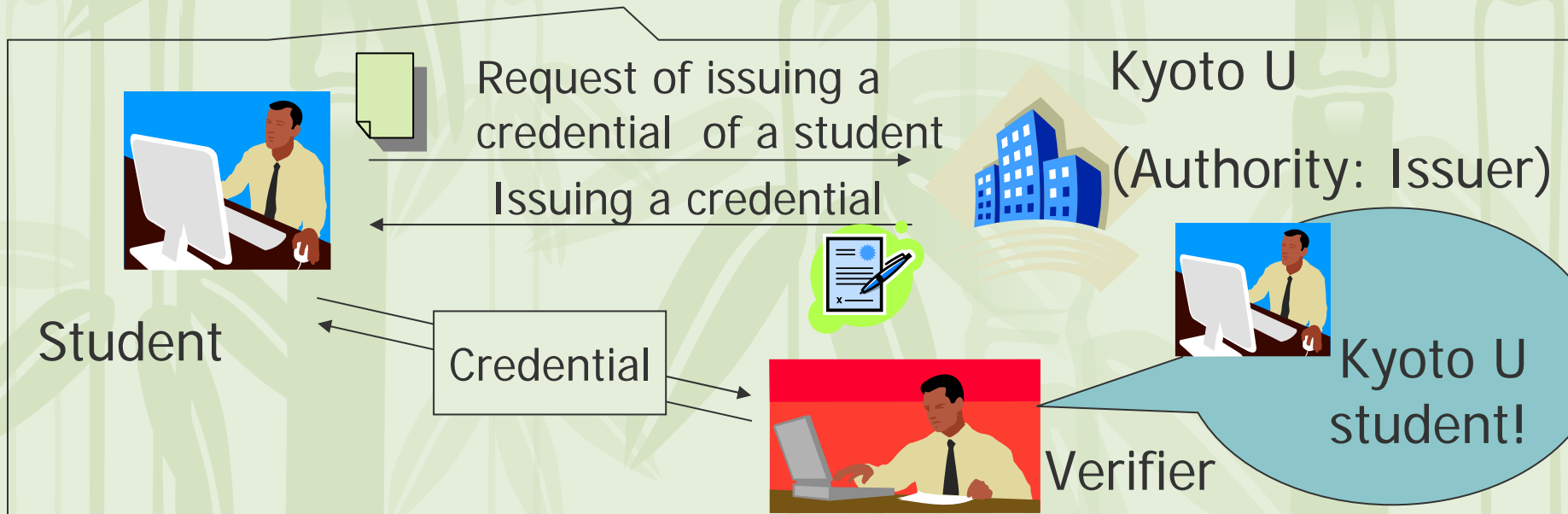
Tatsuaki Okamoto (Kyoto University, NTT Laboratories)

Anonymous Credential

❖ Credential ?

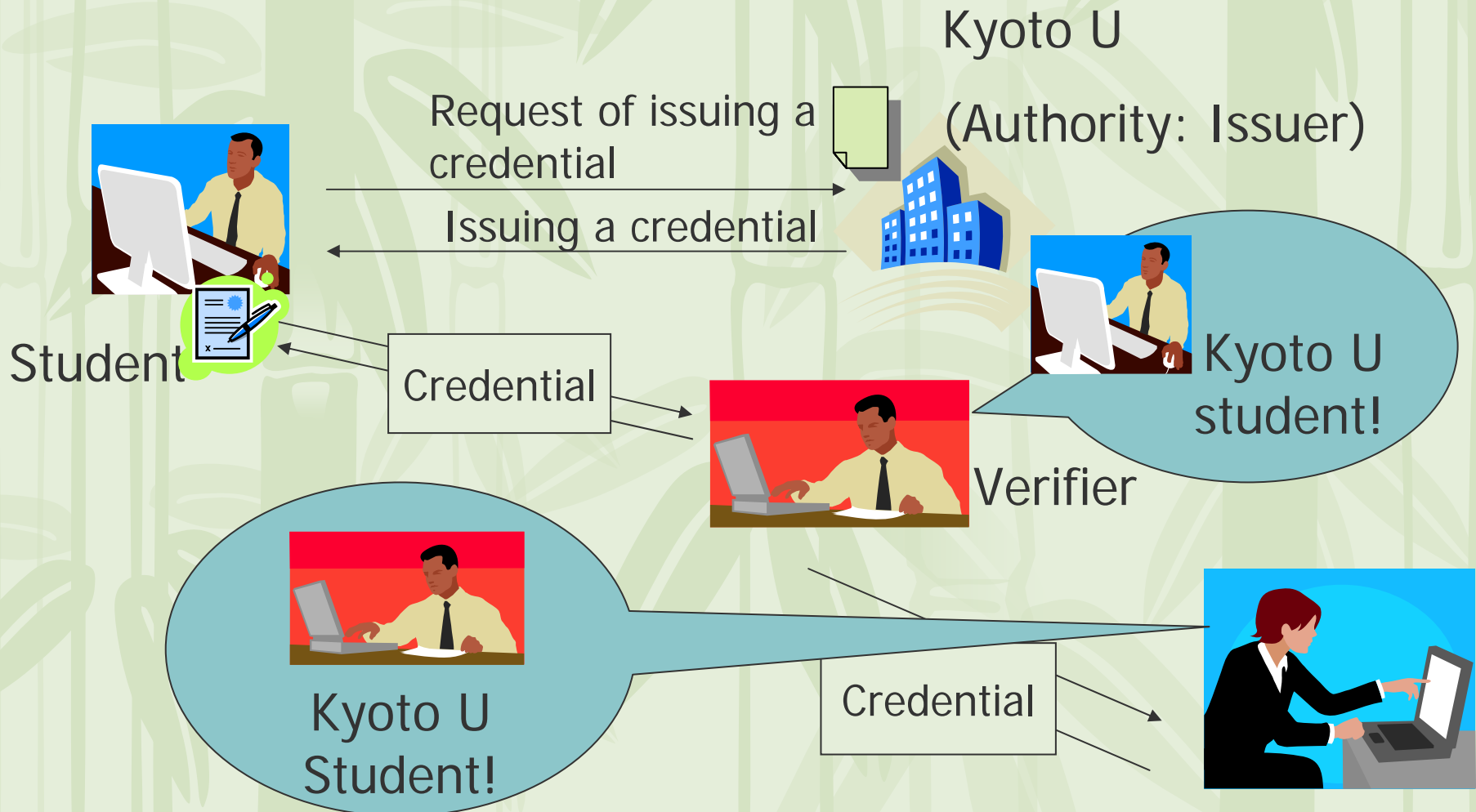
❖ Certificate for person's qualification/attribute

❖ Eg.) “Student of Kyoto U”, “Right to enter a room”



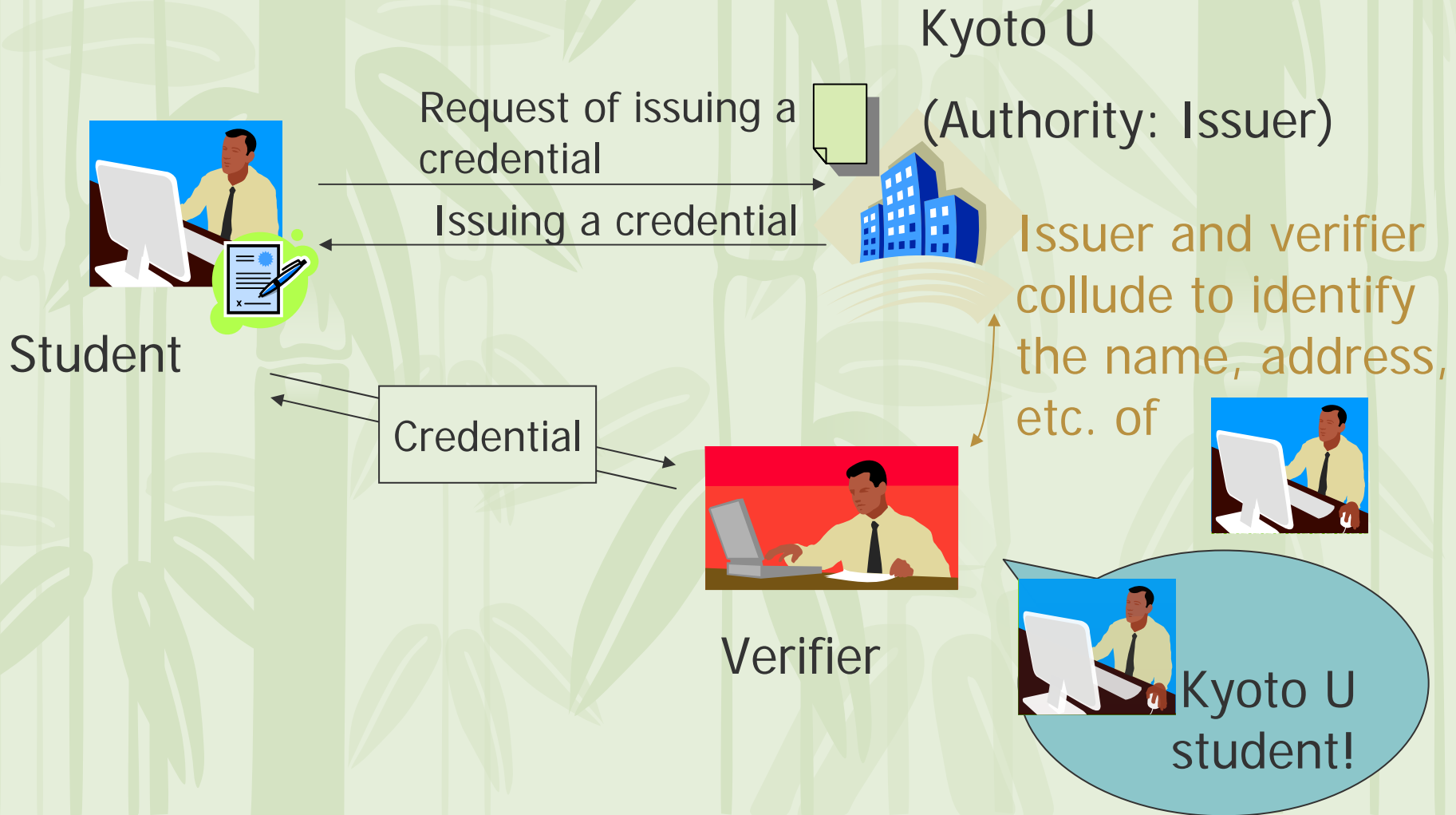
Problem of a system(1)

-Unforgeability

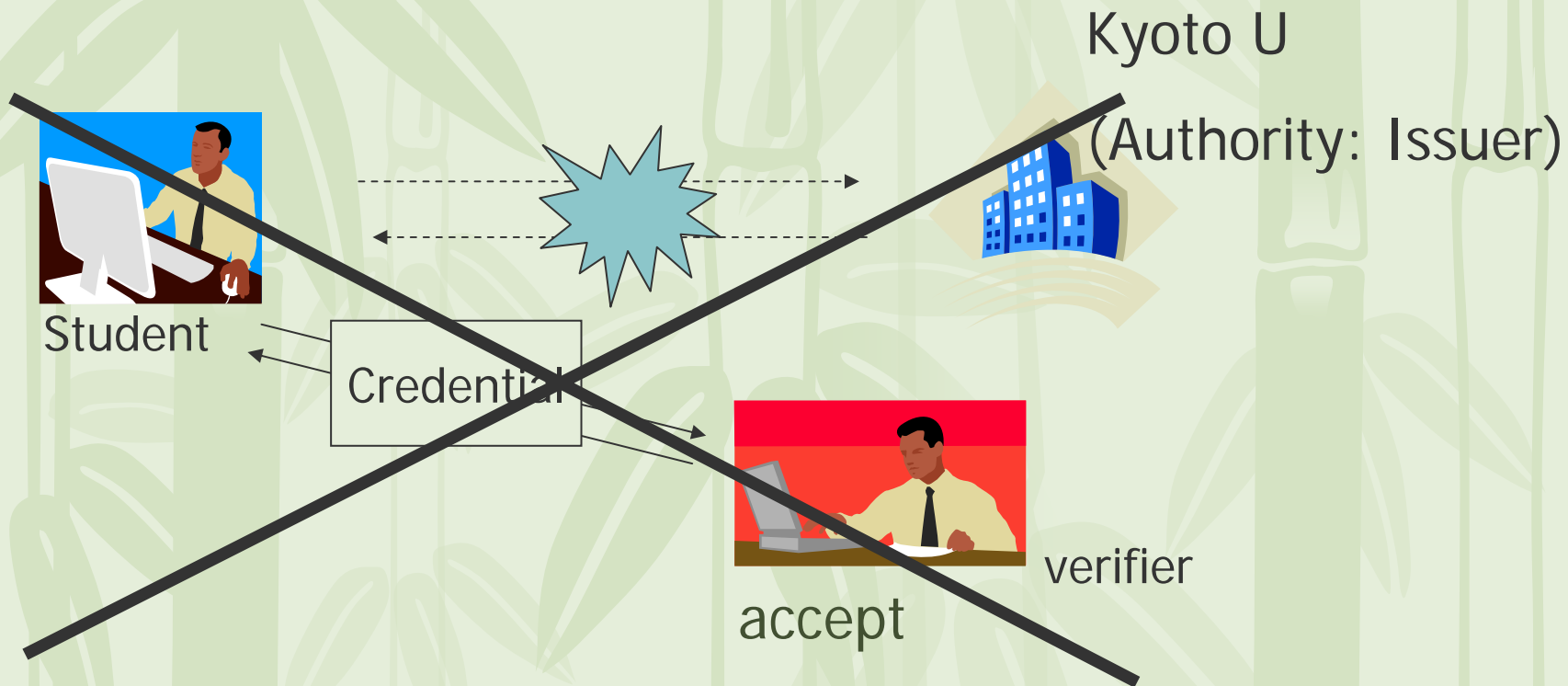


Problem of a system(2)

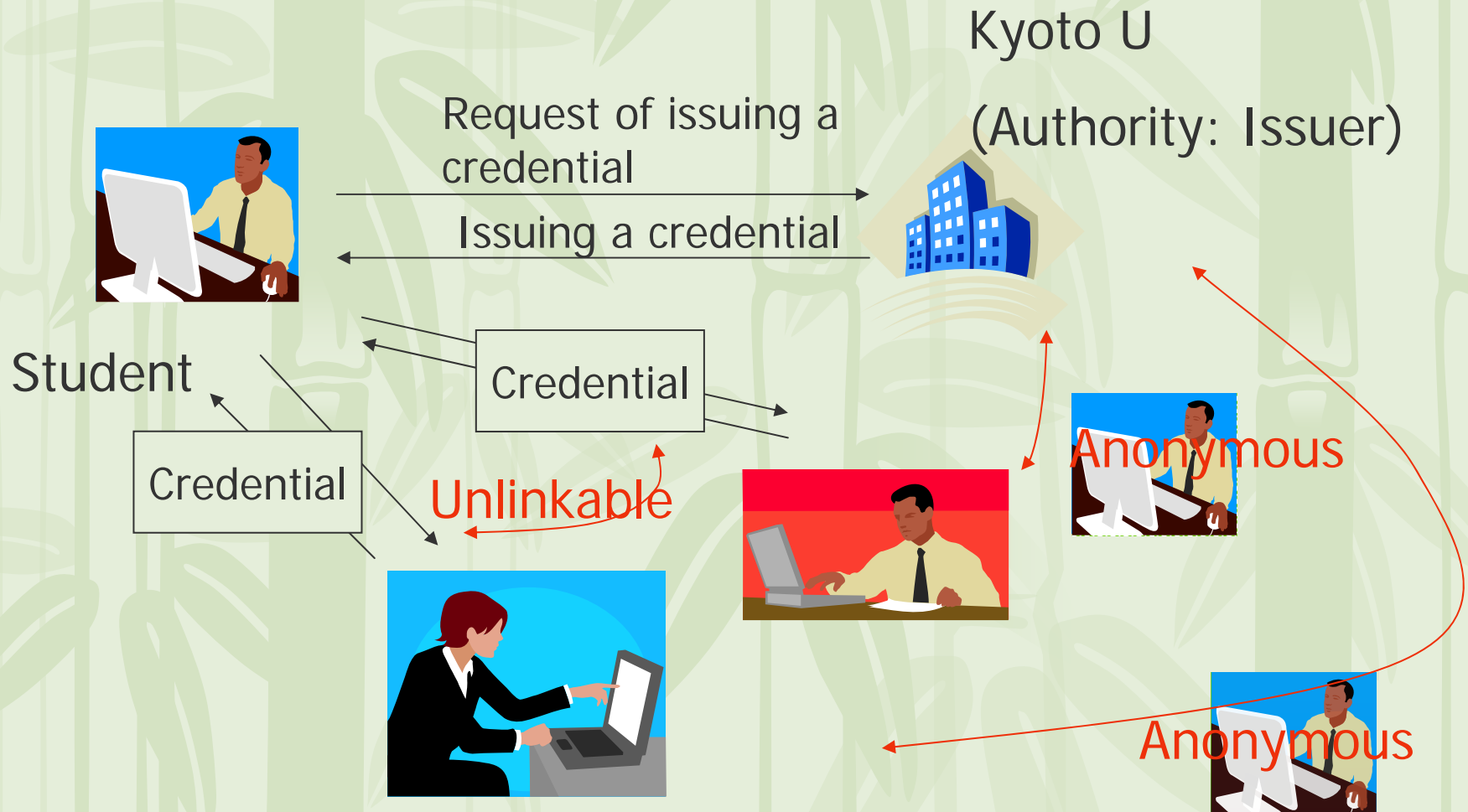
-Privacy



Desirable Properties of a system(1) -Unforgeability



Desirable Properties of a system(2) –Anonymity&Unlinkability



Desirable Properties of a system(3) –Blacklist of Users

❖ Revocation of Credentials

❖ case1-Blacklistable



Desirable Properties of a system(4) –Identity Revealing

❖ Revocation of Credentials

❖ case2-Revealing Identity of bad users

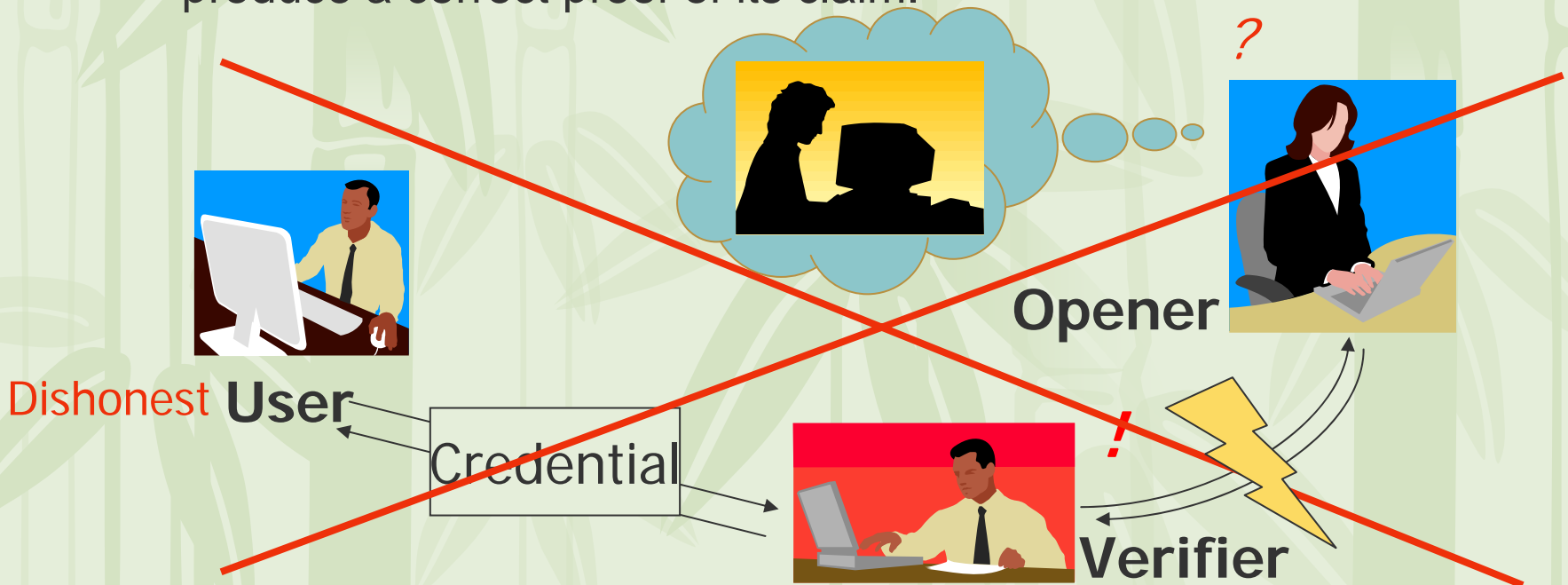


Additional Security Property on the System with Revocation(1)

❖ Traceability

User cannot produce a credential such that

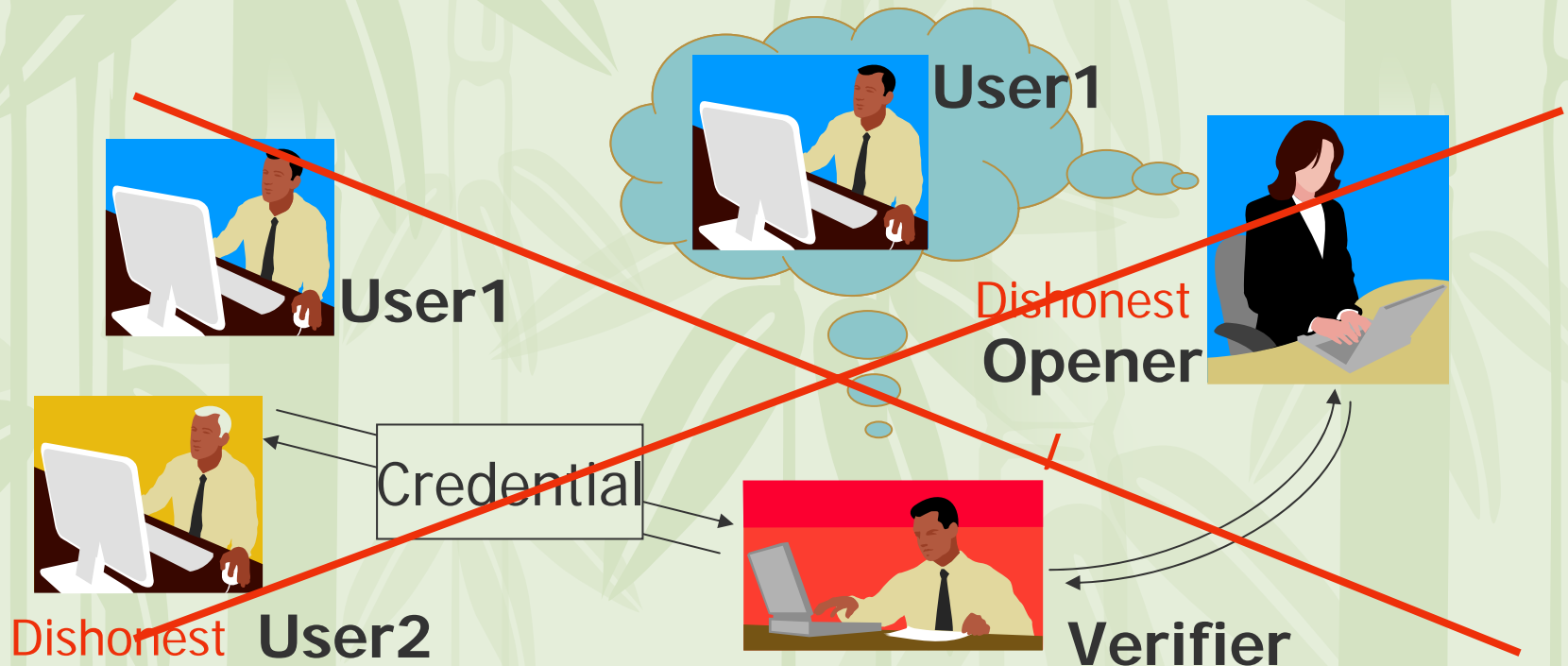
- ❖ Opener cannot identify the origin
- ❖ Opener believes it has identified the origin but is unable to produce a correct proof of its claim.



Additional Security Property on the System with Revocation(2)

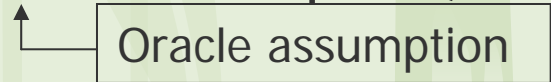
❖ Non-frameability

- ❖ Opener cannot create a proof, accepted by Verifier, that an honest user produced a certain valid proof of the credential unless the user really did produce the proof of the credential.



Related Researches

- ❖ Jan Camenisch and Anna Lysyanskaya
“Signature Schemes and Anonymous Credentials from Bilinear Maps” (CRYPTO2004)
→discrete log based (under LRSW assumption)

Oracle assumption
- ❖ Jan Camenisch and Anna Lysyanskaya
“An efficient non-transferable anonymous multi-show credential system with optional anonymity revocation” (EUROCRYPTO2001)
→strong RSA based, identity revealing function

Related Researches

❖ Patrick Tsang, Man Ho Au, Apu Kapadia,
and Sean Smith

"Blacklistable anonymous credentials:
Blocking misbehaving users without TTPs. "
(CCS2007)

→ revocation(Blacklistable) function

Our Results

- ❖ We construct two anonymous credential systems(SDH assumption based).
- ❖ Basic system
 - without revocation function
 - perfect-anonymity-and-unlinkability
- ❖ System with Revocation
 - with two ways of revocation (blacklistable, credential revealing)
 - computational-anonymity-and-unlinkability

Bilinear Groups

1. G_1 and G_2 are two cyclic groups of prime order p .
2. g_1 : generator of G_1 , g_2 : generator of G_2
3. ψ : isomorphism from G_2 to G_1 , with $\psi(g_2)=g_1$
4. $e: G_1 \times G_2 \rightarrow G_T$, where $|G_1|=|G_2|=|G_T|=p$
 - ... non - degenerate bilinear map
 - $e(u^a, v^b) = e(u, v)^{ab}$ for $u \in G_1, v \in G_2$
 - $e(g_1, g_2) \neq 1$
5. e , ψ , group action in G_1, G_2, G_T can be efficiently computed

Our Basic Anonymous Credential System

❖ Key Generation

User



Authority



$(\mathbb{G}_1, \mathbb{G}_2)$: bilinear groups

ψ : isomorphism from \mathbb{G}_2 to \mathbb{G}_1

$g_2, u_2, v_2 \in_R \mathbb{G}_2$

$g_1 \leftarrow \psi(g_2), u_1 \leftarrow \psi(u_2), \text{ and } v_1 \leftarrow \psi(v_2)$

$x \in_R \mathbb{Z}_p^*$, compute $w_2 \leftarrow g_2^x \in \mathbb{G}_2$

Public key: g_1, g_2, w_2, u_2, v_2

Secret key: x

Our Basic Anonymous Credential System

❖ Credential Issuing

Request to issue a credential
on qualification m

User



Authority



m

$$\sigma \leftarrow \left(g_1^m u_1 v_1^s \right)^{\frac{1}{x+r}}$$

r, s

Public key: g_1, g_2, w_2, u_2, v_2
Secret key: x

Verification

$$e(\sigma, w_2 g_2^r) = e(g_1, g_2^m u_2 v_2^s)$$

Our Basic Anonymous Credential System

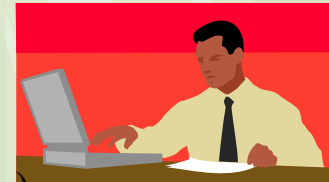
❖ Showing Anonymous Credential

Shows a randomized credential and proves the correctness by WI three-move protocols

User



Verifier



$$\sigma \leftarrow \left(g_1^m u_1 v_1^s \right)^{\frac{1}{x+r}}$$

r, s

$$\sigma' \leftarrow \sigma^{\frac{t}{\theta}} = \left(g_1^m u_1 v_1^s \right)^{\frac{t}{\theta}(x+r)},$$

$$\alpha \leftarrow \left(w_2 g_2^r \right)^{\theta},$$

$$\beta \leftarrow \left(g_2^m u_2 v_2^s \right)^t.$$

$$t \in_R Z_p^*, \theta \in_R Z_p^*$$

$$e(\sigma', \alpha) = e(g_1, \beta)$$

WI - Proof of knowledge of $(\theta \neq 0, r\theta)$ for $\alpha = w_2^\theta g_2^{r\theta}$,

and $(t \neq 0, st)$ for $\beta = (g_2^m)^t u_2^t v_2^{st}$

Security of Our Basic System

- ❖ Unforgeability
 - ❖ computational
 - ❖ SDH assumption

- ❖ Anonymity and Unlinkability
 - ❖ information-theoretical

Efficiency of Our Basic System

	CL04	Ours
Assumption	LRSW	SDH
Size of pk	7 elements	5 elements
Size of sk	3 elements	1 element
Size of Cred	5 elements	3 elements
Size of Proof	4 elements	17 elements
Ops to Issue	5 exp	1 exp
Ops to Verify	8 pairings+2exp	2 pairings+2exp
Ops to Prove	8 pairings+7exp	2 pairings+15exp

Our Anonymous Credential System With Revocation

❖ Key Generation

User



SK: $q \in \mathbb{Z}_p^*, SK_U$
PK: PK_U

SK: $\xi_1, \xi_2 \in \mathbb{Z}_v^*$

PK: $U \leftarrow g_2^{\xi_1}, V \leftarrow g_2^{\xi_2}$

Opener



Authority

$(\mathbb{G}_1, \mathbb{G}_2)$: bilinear groups

ψ : isomorphism from \mathbb{G}_2 to \mathbb{G}_1

$g_2, u_2, v_2 \in_R \mathbb{G}_2$

$g_1 \leftarrow \psi(g_2), u_1 \leftarrow \psi(u_2), \text{ and } v_1 \leftarrow \psi(v_2)$

$x \in_R \mathbb{Z}_p^*$, compute $w_2 \leftarrow g_2^x \in \mathbb{G}_2$

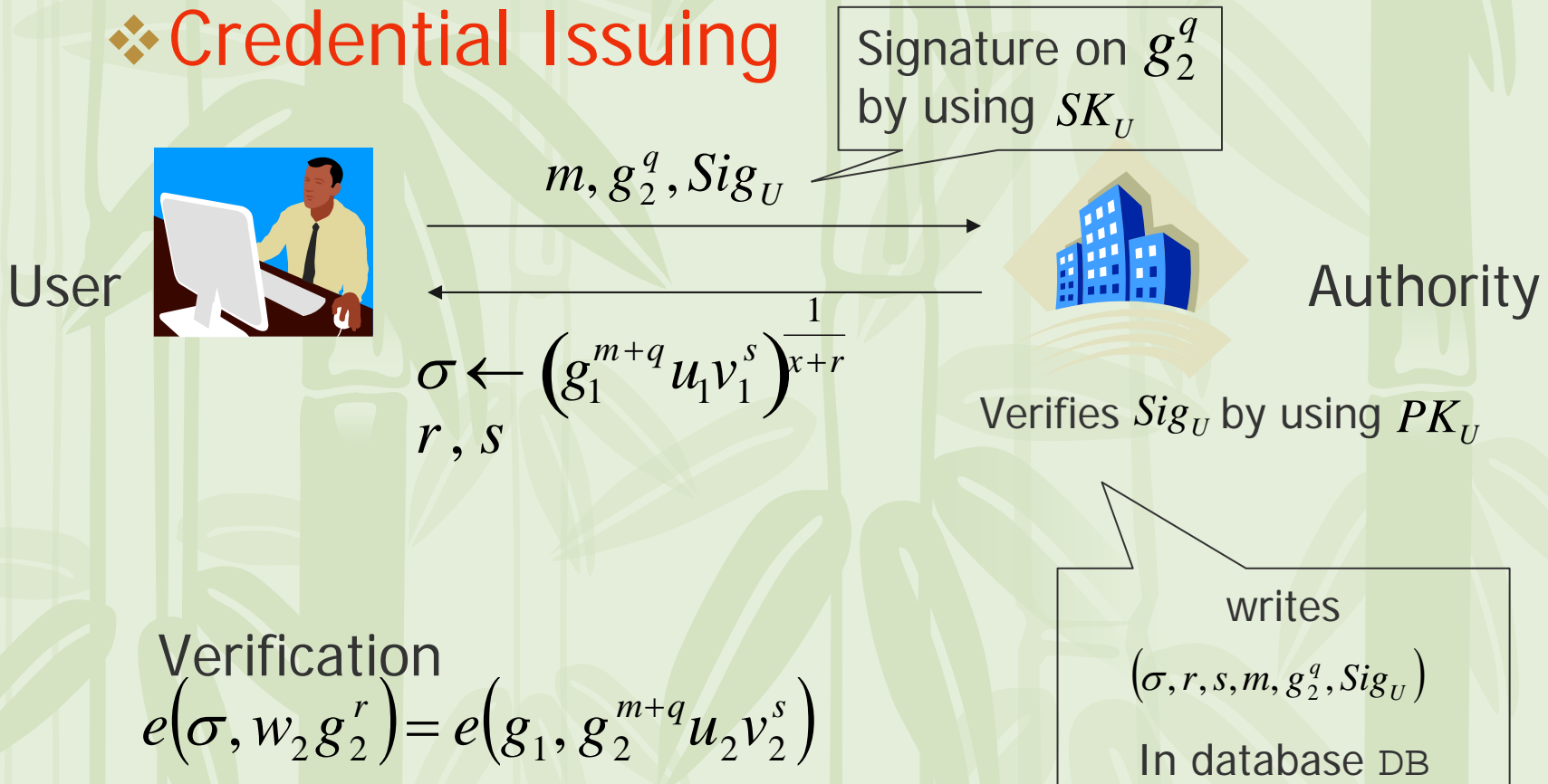
$g, h \in \mathbb{G}_2$

Public key: $g_1, g_2, w_2, u_2, v_2, g, h$

Secret key: x

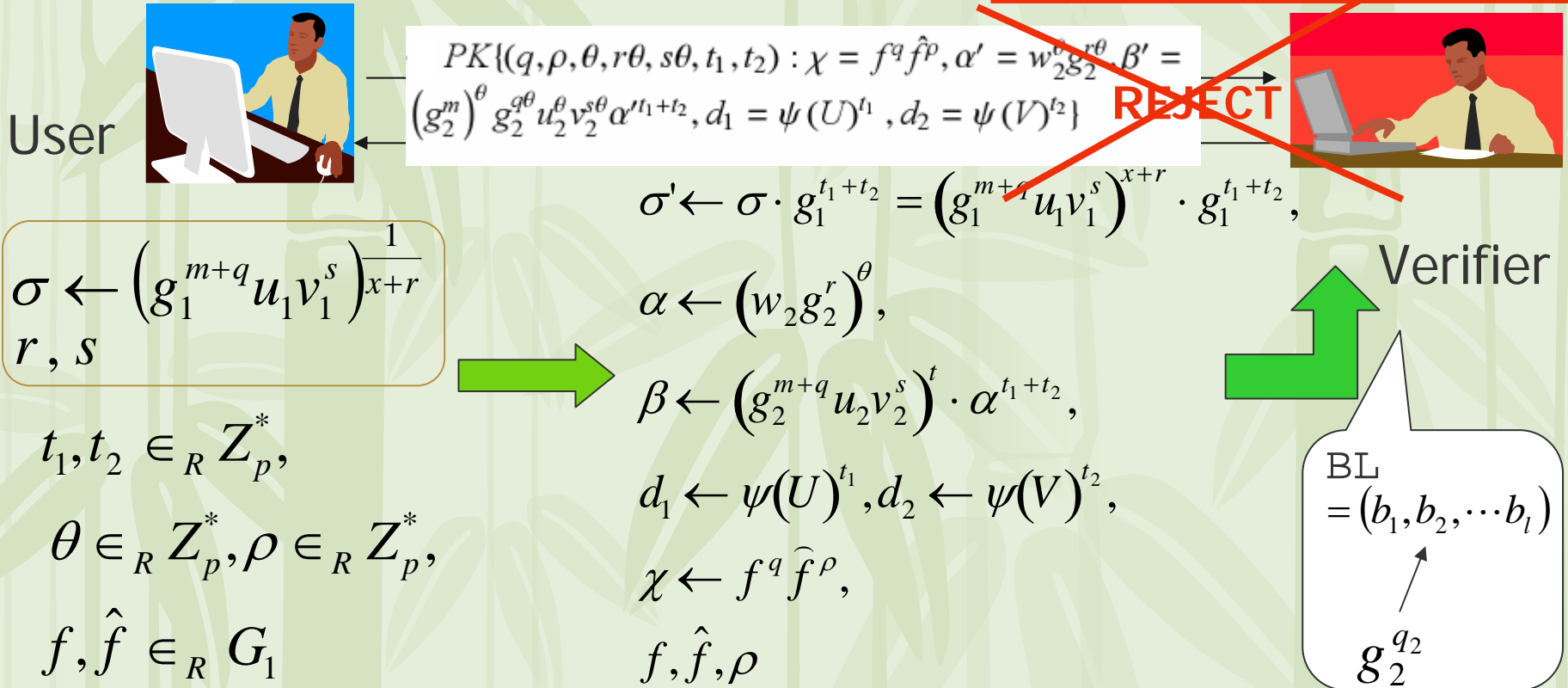
Our Anonymous Credential System With Revocation

❖ Credential Issuing



Our Anonymous Credential System With Revocation

❖ Showing Anonymous Credential **Blacklistable** $e(\sigma', \alpha) = e(g_1, \beta)$
 $e(\chi, g_2) \stackrel{?}{\neq} e(f, b_i) e(\hat{f}, g_2^\rho)$



Our Anonymous Credential System With Revocation

❖ Revealing Identity of a bad user



User

$$\sigma' \leftarrow \sigma \cdot g_1^{t_1+t_2} = (g_1^{m+q} u_1 v_1^s)^{x+r} \cdot g_1^{t_1+t_2},$$

$$\alpha \leftarrow (w_2 g_2^r)^\theta,$$

$$\beta \leftarrow (g_2^{m+q} u_2 v_2^s)^t \cdot \alpha^{t_1+t_2},$$

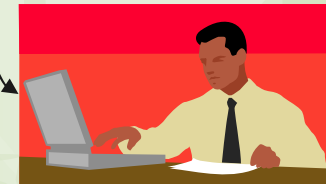
$$d_1 \leftarrow \psi(U)^{t_1}, d_2 \leftarrow \psi(V)^{t_2}$$

$$\sigma = \frac{\sigma'}{d_1^{\frac{1}{\xi_1}} d_2^{\frac{1}{\xi_2}}}$$

$(r, s, m, g_2^q, \text{Sig}_U)$
from DB



Opener



Verifier

$$PK\{(\xi_1, \xi_2) : U = g_1^{\xi_1}, \\ V = g_2^{\xi_2}, \sigma = \sigma' / (d_1^{1/\xi_1} d_2^{1/\xi_2})\}$$

$$e(\sigma', \alpha) = e(g_1, \beta) \text{ checks } \text{Sig}_U \text{ by using } PK_U$$

Efficiency of Our System with Revocation

	CL01	Ours
Assumption	strong RSA, DDH	SDH
Size of pk	10 elements ($ N $)	8 elements ($ p $)
Size of sk	7 elements ($ N $)	5 element ($ p $)
Size of Cred	3 elements ($ N $)	3 elements ($ p $)
Size of Proof	9 elements ($ N $)	42 elements ($ p $)
Size of Open	15 elements ($ N $)	15 elements ($ p $)
Ops to Issue	1 exp (N)	4 exp (p)
Ops to Verify	1 exp (N)	4 exp (p)
Ops to Prove	9 exp (N)	2exp, $l+2$ pairings (p) (l : Blacklisted users)
Ops to Reveal	14 exp (N)	12 exp, 2 pairing (p)

Security of Our System with Revocation

- ❖ Unforgeability

- ❖ computational
- ❖ SDH assumption

- ❖ Anonymity and Unlinkability

- ❖ computational, except for the Opener
- ❖ DDL assumption

Security of Our System with Revocation

- ❖ Treaceability

- ❖ computational

- ❖ SDH assumption

- ❖ Non-frameability

- ❖ computational

- ❖ SDH assumption

Conclusion

- ❖ Two anonymous credential systems
 - ❖ The Basic system
 - ❖ information-theoretically anonymous-and-unlinkable
 - ❖ The System with revocation
 - ❖ Blacklistable, Identity Revealing
- ❖ Proofs of Security
- ❖ Comparison of Efficiency