Efficient Certificateless Signcryption

Diego Aranha, Rafael Castro, Julio López, Ricardo Dahab

Institute of Computing - UNICAMP

Funded by FAPESP, Grant No. 2007/06950-0

The problem

Providing confidentiality, authentication and non-repudiation to a message...

Solution: Encrypt and sign!

...in a single efficient operation, preventing external influences.

Solution: Signcrypt!

Public key cryptography models

Public Key Infrastructures (PKI)

- Certificate authority issues certificates;
- Users verify public key certificates;
- Problem: High computational and storage requirements.

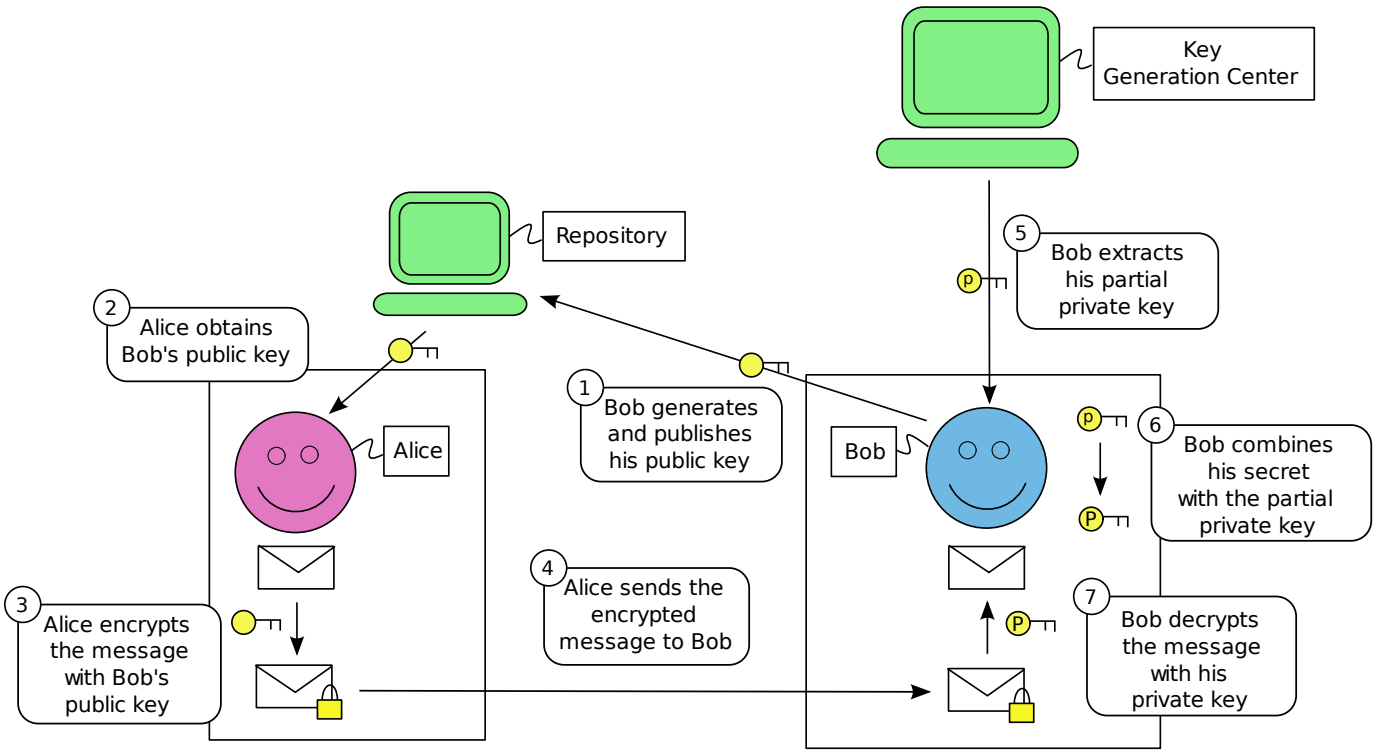
Identity-Based Cryptography (ID-PKC)

- Central authority (PKG) generates private keys;
- Public keys are identities (easy verification);
- Problem: Private key escrow.

Certificateless Public Key Cryptography (CL-PKC)

- Central authority (KGC) issues partial private keys;
- Users combine partial keys with their own secrets;
- Advantages: No key escrow and reduced costs.

Certificateless Public Key Cryptography



CL-PKC Signcryption

There is already a CL-PKC signcryption protocol with a security reduction [Barbosa and Farshim], but it's not very efficient.

Contribution

Efficient protocol for signcryption under the Certificateless Public Key Cryptography model.

Bilinear pairings

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be additive groups such that $|\mathbb{G}_1| = |\mathbb{G}_2| = q$ and $\mathbb{G}_T$ be a multiplicative group of order q. Let P be the generator of $\mathbb{G}_1$ and Q the generator of $\mathbb{G}_2$.

A map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is an *admissible bilinear pairing* if it satisfies:

1. *Bilinearity:* given $(V, W) \in \mathbb{G}_1 \times \mathbb{G}_2$ and $(a, b) \in \mathbb{Z}_q$, we have $e(aV, bW) = e(V, W)^{ab} = e(abV, W) = e(V, abW)$.
2. *Non-degeneracy:* $e(P, Q) \neq 1_{\mathbb{G}_T}$.
3. *Efficiency:* the map can be computed efficiently.

Proposed CL-PKC Signcryption

Let $y_E \in \mathbb{Z}_q^* = H_1(\mathrm{ID}_E)$.

- **Setup:** KGC generates master key s, publishes $P \in \mathbb{G}_1, Q \in \mathbb{G}_2, g = e(P, Q)$ and $P_{pub} = sP$;
- **Extract:** For user E, KGC issues the partial private key $D_E = (s + y_E)^{-1} Q$;
- **Keygen:** User E generates secret x_E and computes its private key $S_E = x_E^{-1} D_E$ and public key $P_E = x_E(P_{pub} + y_E P)$.

We have $e(P_E, S_E) = g$.

Proposed CL-PKC Signcryption

User A wants to signcrypt m for B.

- **Signcrypt:**
  A selects $r \in \mathbb{Z}_q^*$ and encrypts $C = m \oplus H_2(g^{r^{-1}})$;
  A computes $h = H_3(C, rP_A, \mathrm{ID}_A, r^{-1}P_B, \mathrm{ID}_B)$;
  A signs $T = (r + h)^{-1} S_A$;
  A sends $(C, rP_A, r^{-1}P_B, T)$ to B.

- **Unsigncrypt:**
  B receives (C, R, S, T);
  B computes $h' = H_3(C, R, \mathrm{ID}_A, S, \mathrm{ID}_B)$;
  B decrypts $m' = C \oplus H_2(e(S, S_B))$;
  If $e(R + h'P_A, T) = g$, B accepts m'.

Efficiency

		Operations				
Algorithm	**Protocol**	e	kP	g^x	a^{-1}	H
Precomp.	[Barbosa and Farshim]	1	0	0	0	0
	Proposed	0	0	0	0	0
Signcrypt	[Barbosa and Farshim]	0	$3 + \sigma^{\dagger}$	1	0	3
	Proposed	0	3	1	2	2
Unsigncrypt	[Barbosa and Farshim]	4	1	0	0	3
	Proposed	2	1	0	0	2

† Two of the scalar multiplications can be simultaneous

Conclusions

The proposed protocol:

- is more efficient than [Barbosa and Farshim];
- is transferable (supports public verification of signcrypted messages);
- does not have a security demonstration yet.

The protocol [Barreto et al.]:

- is more efficient than the proposed protocol but not transferable;
- can be transferable with **equivalent** performance.