Provably Secure Randomized Blind Signature Scheme Based on Bilinear Pairing

Chun-I Fan, Wei-Zhe Sun, and Vincent Shi-Ming Huang

Speaker: Wei-Zhe Sun

Computers & Mathematics with Applications 01/2010; 60(2):285-293.
The final publication is available at http://www.sciencedirect.com

Electronic Commerce & Security Engineering Lab.

Department of Computer Science and Engineering
National Sun Yat-sen University, Kaohsiung, Taiwan

Outline

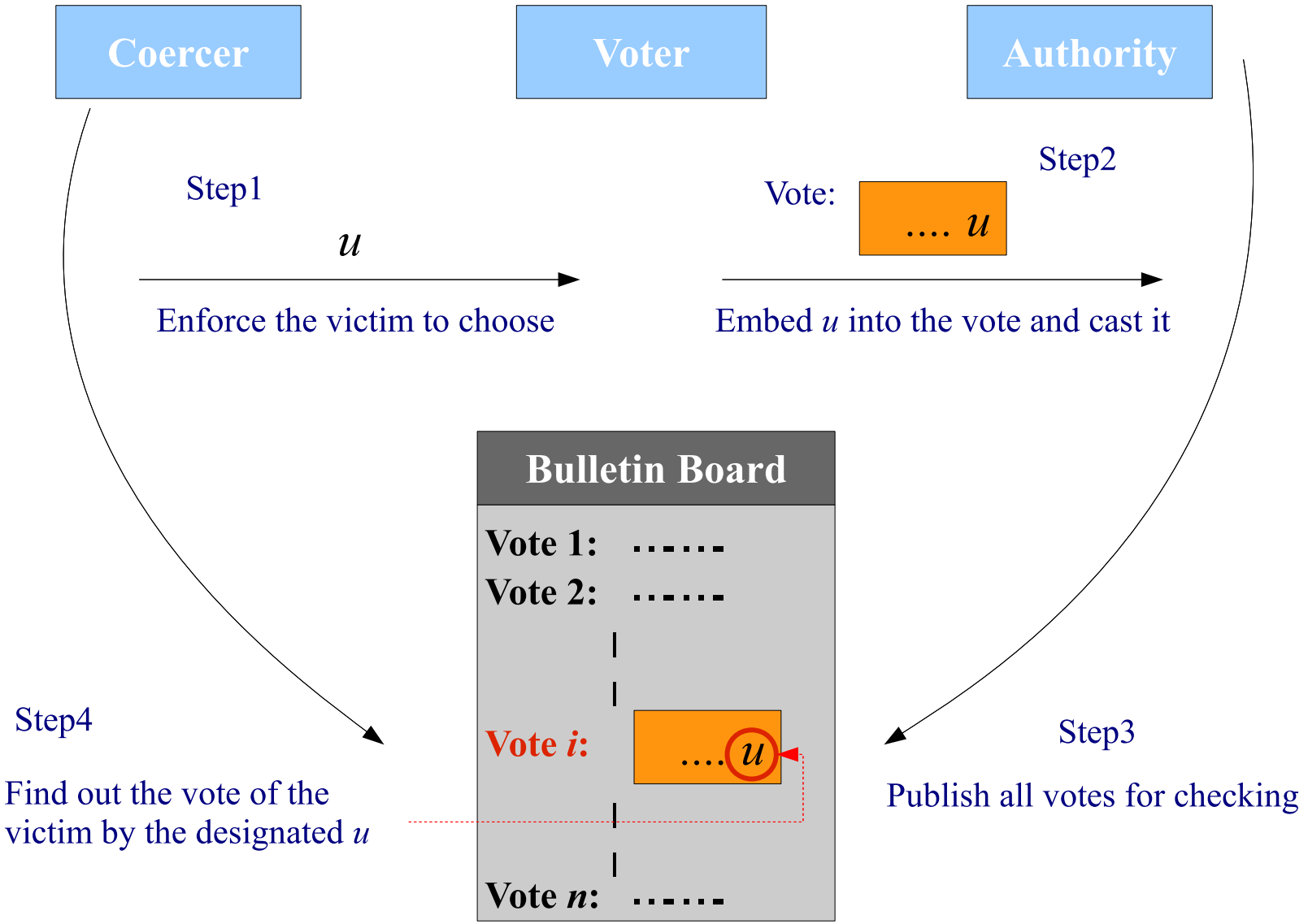
Blind Signature

- This idea was presented by Chaum in 1983.
- A typical blind signature scheme satisfies *unlinkability* and *unforgeability* properties.
- Due to the unlinkability property, it can be applied to various privacy-oriented applications, such as e-payment and anonymous e-voting systems.

Randomization

- ⋆ This property was introduced by Ferguson in 1994 for security concerns in blind signatures.
- ⋆ None of the articles in the literature has formally shown that a blind signature is not secure owing to lack of randomization.
- ⋆ In 2006, Fan et al. has pointed out that the randomization property is an essential property of a blind signature while it is applied to construct e-voting systems against coercion and bribery.

An Example of Coercion



Our Contributions

- ⋆ We come up with a novel blind signature scheme with the randomization property from bilinear pairing primitives.
- ⋆ We pioneer in providing a concrete definition of the randomization property and formally prove it in the standard model.
- ⋆ The proposed scheme is free from the key escrow problem.

Bilinear Map

Let G_1 be a cyclic additive group generated by P and G_2 be a cyclic multiplicative group, where both of them are with the same prime order q. A bilinear map operation $e : G_1 \times G_1 \rightarrow G_2$ satisfies the following three properties.

1. **Bilinearity**: $\forall P, Q \in G_1$ and $\forall a, b \in \mathbb{Z}_q$, $e(aP, bQ) = e(P, Q)^{ab}$.
2. **Non-degeneracy**: $\exists P, Q \in G_1$, such that $e(P, Q) \neq 1$.
3. **Computability**: There exists an efficient algorithm to compute $e(P, Q)$, $\forall P, Q \in G_1$, in polynomial time.

The Proposed Randomized Blind Signature Scheme

$SK = (x_1, x_2)$
$PK = (x_1P, x_2P)$

User	Signer
$u, r_1, r_2 \in_R \mathbb{Z}_q^*$	$y \in_R \mathbb{Z}_q^*$
	yP ←
$C = uyP$	
$\alpha_1 = r_1 H(m\|\|C) + r_2 P$	
$\alpha_2 = r_1 u \pmod q$	
(α_1, α_2) →	
	$T = x_1\alpha_1 + x_2 y \alpha_2 P$
	T ←
$S = r_1^{-1}(T - r_2 Pub_1)$	

Signature-message tuple: (S, m, C)

Verification: $e(S, P) \stackrel{?}{=} e(H(m||C), Pub_1)e(C, Pub_2)$

Theorem (Correctness of $\mathcal{RBSB}$)

$\mathcal{RBSB}$ satisfies correctness.

Proof:
Given a signature-message triple (S, m, C) produced from $\mathcal{RBSB}$, it satisfies

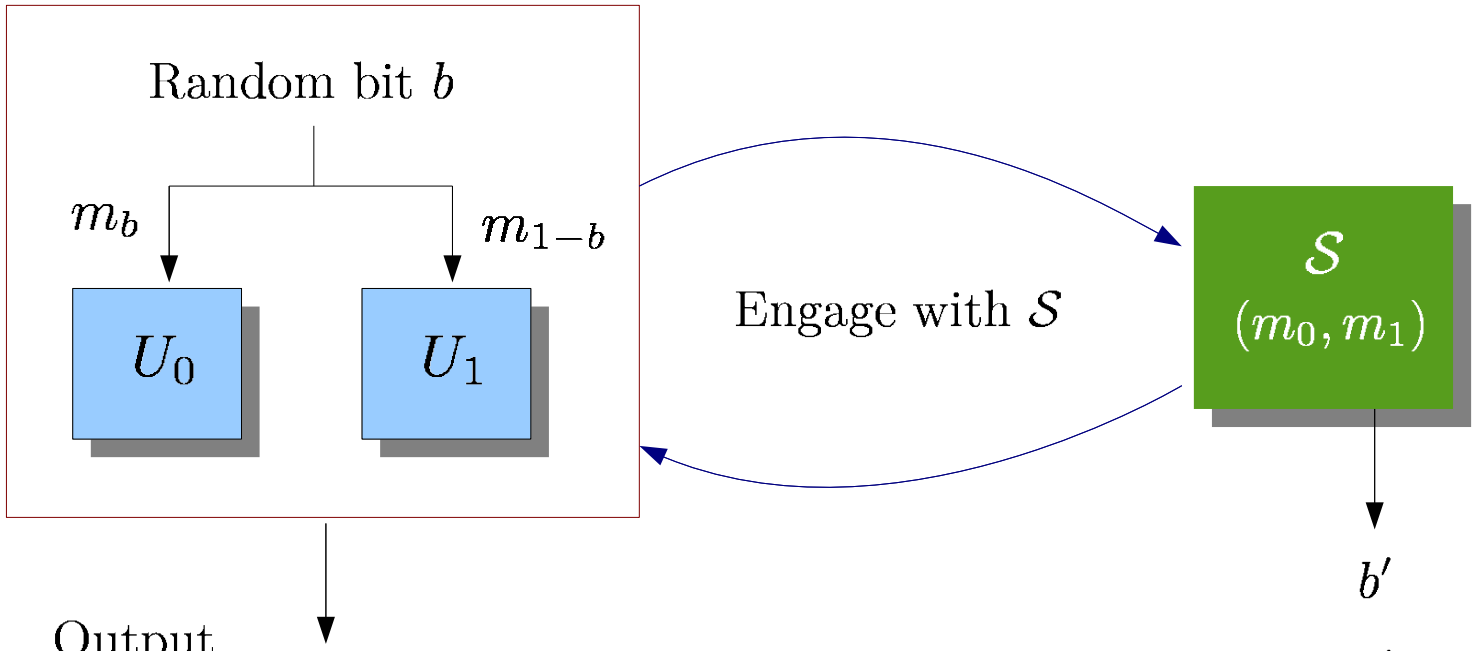
$$e(S,P) = e(r_1^{-1}(x_1\alpha_1 + x_2 y\alpha_2 P - r_2 P u b_1), P)$$

$$= e(r_1^{-1}(x_1 r_1 H(m||C) + r_2 x_1 P + x_2 y r_1 u P - r_2 P u b_1), P)$$

$$= e(x_1 H(m||C) + x_2 u y P, P) = e(x_1 H(m||C), P) e(x_2 u y P, P)$$

$$= e(H(m||C), P u b_1) e(C, P u b_2)$$

Linkage Game



The advantage of $\mathcal{S}$ is

$$\mathbf{Adv}^{Link}_{\mathcal{RBS}}(\mathcal{S}) = |2Pr[b' = b] - 1|$$

Definition (Unlinkability)

A randomized blind signature scheme satisfies the unlinkability property if the advantage of $\mathcal{S}$ winning the linkage game is negligible.

Theorem (Unlinkability of $\mathcal{RBSB}$)

$\mathcal{RBSB}$ satisfies the unlinkability property.

Proof:

- ⋆ Let $(y_i, \alpha_{1_i}, \alpha_{2_i}, T_i)$ be the view of parameters exchanged during the signature protocol to $\mathcal{S}$ corresponding to instance i.
- ⋆ Given a signature-message triple $(S, m, C) \in \{(S_0, m_0, C_0), (S_1, m_1, C_1)\}$, for any view $(y_i, \alpha_{1_i}, \alpha_{2_i}, T_i)$, $i \in \{0, 1\}$, there always exists a corresponding triple $(r'_{1_i}, r'_{2_i}, u'_i)$ such that

$$C = u'_i y_i P$$

and

$$\begin{cases} \alpha_{2_i} = r'_{1_i} u'_i \pmod q \\ \alpha_{1_i} = r'_{1_i} H(m||C) + r'_{2_i} P. \end{cases}$$

- We get

$$
\begin{aligned}
& S \\
&= {r'_{1_i}}^{-1}(T_i - r'_{2_i} Pub_1) \\
&= {r'_{1_i}}^{-1}(x_1 \alpha_{1_i} + x_2 y_i \alpha_{2_i} P - r'_{2_i} Pub_1) \\
&= {r'_{1_i}}^{-1}(x_1(r'_{1_i} H(m||C) + r'_{2_i} P) + x_2 y_i r'_{1_i} u'_i P - r'_{2_i} Pub_1) \\
&= {r'_{1_i}}^{-1}(x_1 r'_{1_i} H(m||C) + x_2 y_i r'_{1_i} u'_i P) \\
&= x_1 H(m||C) + x_2 y_i u'_i P \\
&= x_1 H(m||C) + x_2 C
\end{aligned}
$$

  and thus it implies that the verification formula always holds.

- From above, the signer $\mathcal{S}$ succeeds in determining b with probability only $\frac{1}{2}$, and we have $\mathbf{Adv}^{Link}_{\mathcal{RBS}}(\mathcal{S}) = 0$.

  Therefore, $\mathcal{RBSB}$ possesses the unlinkability property.

Definition (The Chosen-Target CDH Assumption)

Let G be a group with prime order q generated by P. An adversary $\mathcal{A}$ is given (P, aP), where $a \in_R \mathbb{Z}_q$, and $\mathcal{A}$ is allowed to access the following two kinds of oracles

Oracle $\mathcal{TO}()$	Oracle $\mathcal{HO}(Z)$
1. Select $Z \in_R G$;	1. Compute $V = aZ$;
2. Return Z;	2. Return V;

$\mathcal{A}$ wins the game if $\mathcal{A}$ can output ℓ pairs $\{(V_1, Z_1), \ldots, (V_\ell, Z_\ell)\}$, $q_h < \ell \leq q_t$, such that $V_i = aZ_i$ $(1 \leq i \leq \ell)$ after making q_t $\mathcal{TO}$ queries to obtain $(Z_1, \ldots, Z_{q_t}) \in G^{q_t}$ and q_h $\mathcal{HO}$ queries $(q_h < q_t)$.

This assumption states that there exists no probabilistic polynomial-time adversary $\mathcal{A}$ who can win the above game with non-negligible probability.

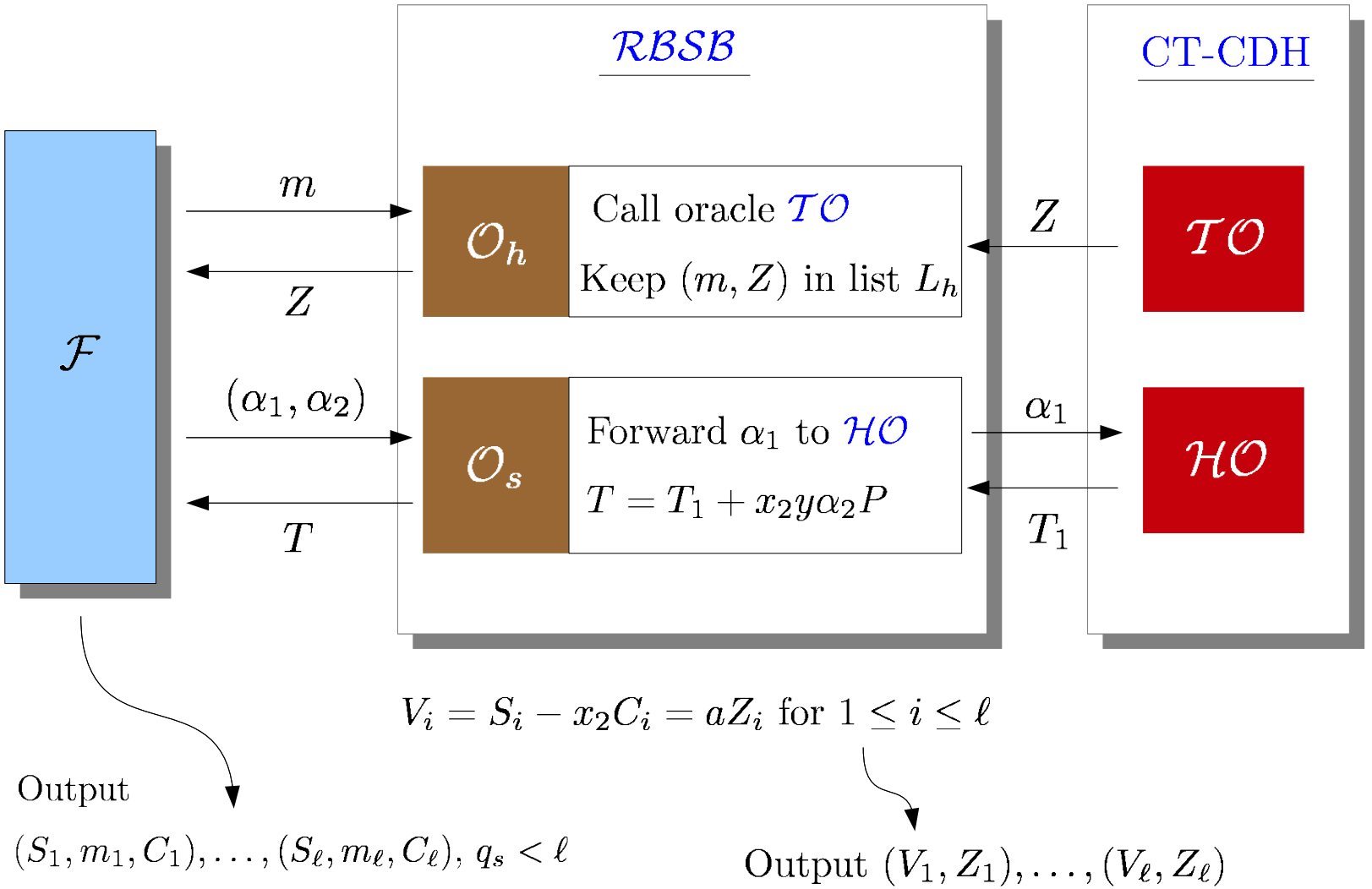
Theorem (Unforgeability of $\mathcal{RBSB}$)

$\mathcal{RBSB}$ is secure against one-more forgery under the Chosen-Target CDH assumption.

Proof:

- Let (P, aP) be the challenge from the Chosen-Target CDH assumption.
- Set $(q, H, G_1, G_2, e, P, Pub_1, Pub_2)$ be the public system parameters of $\mathcal{RBSB}$ where $Pub_1 = aP$.

Simulation


$\mathcal{RBSB}$
CT-CDH
$\mathcal{F}$
m
Z
$\mathcal{O}_h$
Call oracle $\mathcal{TO}$
Keep (m, Z) in list L_h
Z
$\mathcal{TO}$
(α_1, α_2)
T
$\mathcal{O}_s$
Forward α_1 to $\mathcal{HO}$
$T = T_1 + x_2 y \alpha_2 P$
α_1
T_1
$\mathcal{HO}$
$V_i = S_i - x_2 C_i = aZ_i$ for $1 \leq i \leq \ell$
Output
$(S_1, m_1, C_1), \ldots, (S_\ell, m_\ell, C_\ell)$, $q_s < \ell$
Output $(V_1, Z_1), \ldots, (V_\ell, Z_\ell)$

Definition (Radomization)

Let (s, m, c) be an instance of valid signature-message triple generated from a blind signature scheme, where m is the plaintext message to be signed, c is the randomization parameter, and s is the signature on (m, c).

Given a random element c', we say that the scheme satisfies the randomization property if there exists no polynomial-time adversary who can output a valid signature-message triple (s, m, c) satisfying $c = c'$ with non-negligible probability.

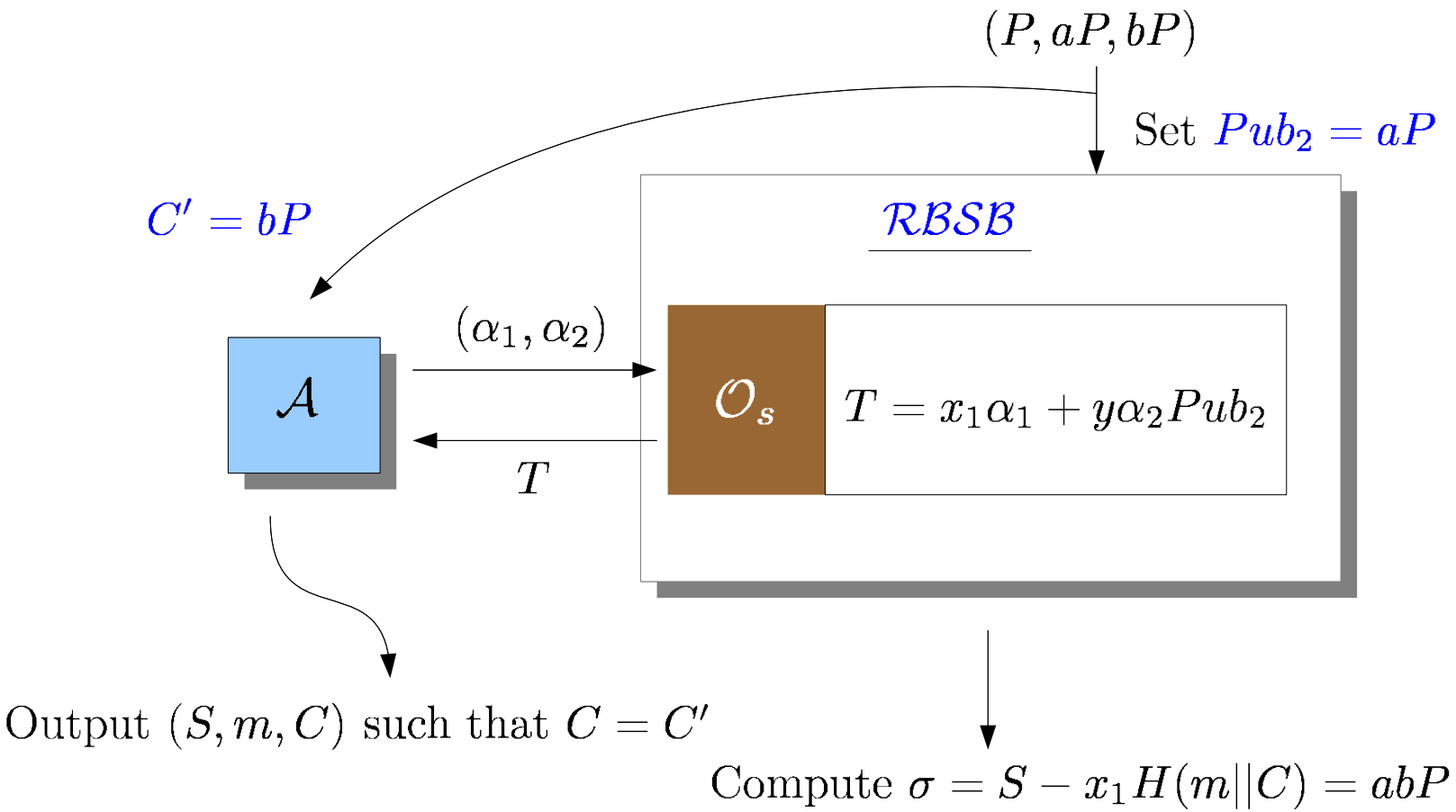
Definition (Computational Diffie-Hellmen (CDH) Problem)

Let G be a cyclic group generated by P with order q. For $a, b \in \mathbb{Z}_q$, given $P, aP, bP \in G$, compute abP.

Theorem (Randomization of $\mathcal{RBSB}$)

In $\mathcal{RBSB}$, given a random element $C' \in G_1$, if there exists a polynomial-time adversary who can produce a valid signature-message triple (S, m, C) satisfying $C = C'$ with non-negligible probability, then we can solve the CDH problem with non-negligible probability.

Simulation


(P, aP, bP)
Set $Pub_2 = aP$
$C' = bP$
$\mathcal{RBSB}$
(α_1, α_2)
$\mathcal{A}$
$\mathcal{O}_s$
$T = x_1\alpha_1 + y\alpha_2 Pub_2$
T
Output (S, m, C) such that $C = C'$
Compute $\sigma = S - x_1 H(m||C) = abP$

Conclusion

1. We have presented a novel construction on a pairing-based blind signature scheme with the randomization property.

2. To the best of our knowledge, the proposed scheme is the first provably secure randomized blind signature scheme from bilinear pairing primitives.


Thanks for Your Attention !!