Block-wise P-Signatures and Non-Interactive Anonymous Credentials with Efficient Attributes

Malika Izabachène[1], Benoit Libert[2] and Damien Vergnaud[3]

[1]ENS Cachan/INRIA/CNRS

[2]Université Catholique de Louvain-la-Neuve

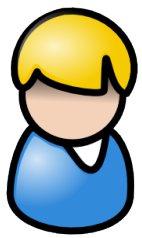
[3]ENS/INRIA/CNRS

Thursday, 15th, December 2011

Credentials

Anonymous credential systems

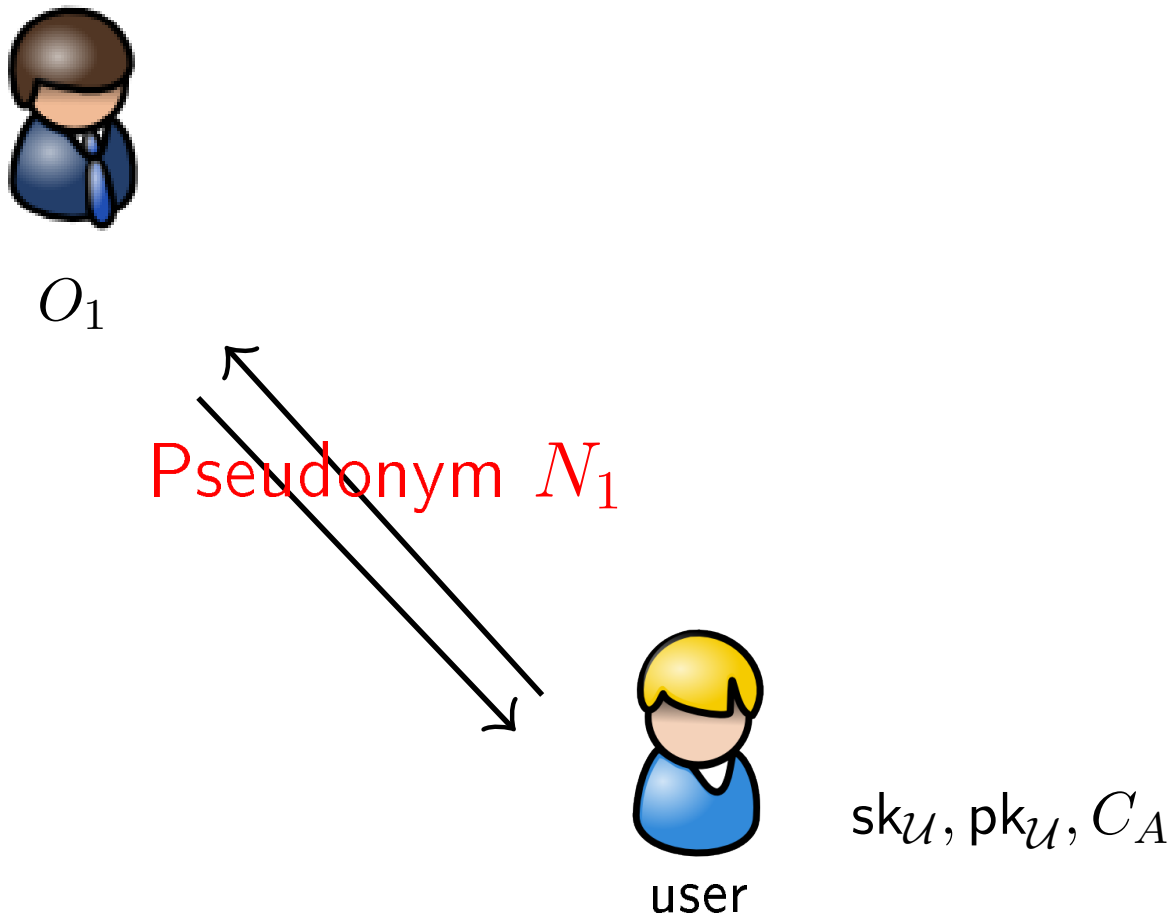
O_1



user

$\mathsf{sk}_{\mathcal{U}}, \mathsf{pk}_{\mathcal{U}}, C_A$

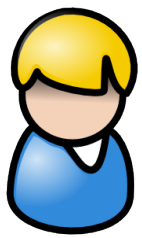
Anonymous credential systems



Anonymous credential systems

O_1

$\mathsf{pk}_1, \mathsf{sk}_1, N_1, com$



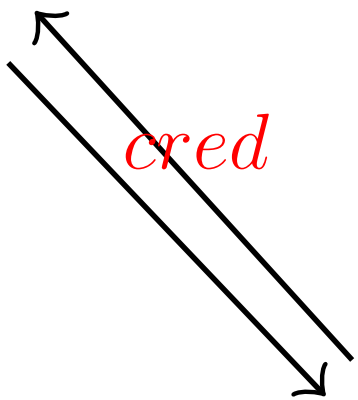
user

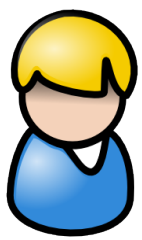
$\mathsf{sk}_{\mathcal{U}}, \mathsf{pk}_{\mathcal{U}}, N_1, \mathsf{aux}_1$

Anonymous credential systems

$\mathsf{pk}_1, \mathsf{sk}_1, N_1, com$

O_1



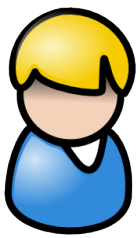


user

$\mathsf{sk}_{\mathcal{U}}, \mathsf{pk}_{\mathcal{U}}, N_1, \mathsf{aux}_1$

Anonymous credential systems

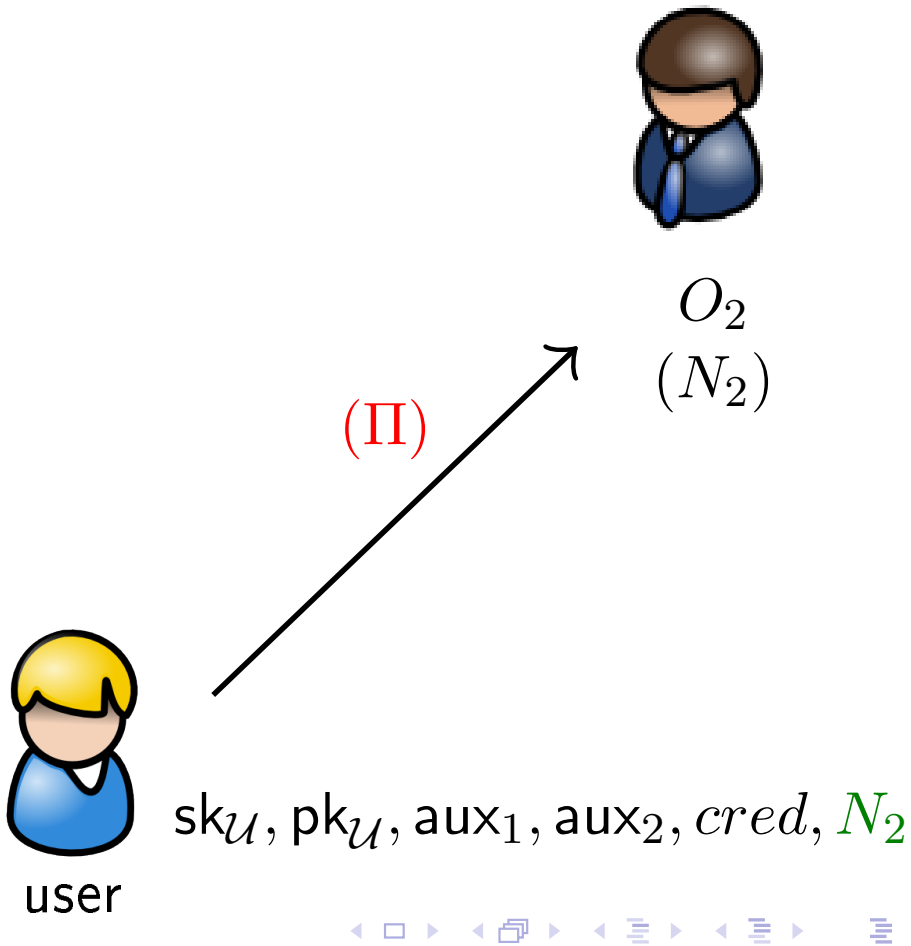
O_2
(N_2)



user

$\mathsf{sk}_{\mathcal{U}}, \mathsf{pk}_{\mathcal{U}}, \mathsf{aux}_1, \mathsf{aux}_2, cred, N_2$

Anonymous credential systems



Anonymous credential systems

$\mathsf{Verify}(\Pi)$

O_2

(N_2)

Main steps

$$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$$

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(m) + m$

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(m) + m$

  provides $\longrightarrow$ Integrity of m

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(m) + m$
  provides $\longrightarrow$ Integrity of m
- Π=Proof of ownership of σ_i on m_i s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, m_i)$

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}=\texttt{"18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(m) + m$

  provides $\longrightarrow$ Integrity of m

- Π=Proof of ownership of σ_i on m_i s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, m_i)$

  provides $\longrightarrow$ Rightness of id

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}=\texttt{"18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(m) + m$

  provides $\longrightarrow$ Integrity of m

- Π=Proof of ownership of σ_i on m_i s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, m_i)$

  provides $\longrightarrow$ Rightness of id

- Proof of ownership of σ_i s.t.
  - $\text{Verify}(\text{pk}_{\text{id}}, \sigma, m_i)$
  - Prove possession of m_i without revealing m_i

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}=\texttt{"18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(m) + m$

  provides $\longrightarrow$ Integrity of m

- Π=Proof of ownership of σ_i on m_i s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, m_i)$

  provides $\longrightarrow$ Rightness of id

- Proof of ownership of σ_i s.t.
  - $\text{Verify}(\text{pk}_{\text{id}}, \sigma, m_i)$
  - Prove possession of m_i without revealing m_i

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}=\texttt{"18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(m) + m$

  provides $\longrightarrow$ Integrity of m

- Π=Proof of ownership of σ_i on m_i s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, m_i)$

  provides $\longrightarrow$ Rightness of id

- Proof of ownership of σ_i s.t.
  - $\text{Verify}(\text{pk}_{\text{id}}, \sigma, m_i)$
  - Prove possession of m_i without revealing m_i

  provides $\longrightarrow$ Anonymous Authentication of pk_{id}

Previous work

- Anonymous Credentials (AC) [Chaum85, Brands95]
- Non-interactive AC from P-signature [BCKL08]
- AC with Selective disclose of attributes [CL01]
  ✗ Each Proof is linear in number of attributes
- AC with a new encoding + More statements [CG10]
  ✓ More efficient and even practical
  ✗ Still based on interactive signature
  - 3-rounds of interaction
  - Security Proof in the RO

$\rightsquigarrow$ Non-interactive Anonymous credentials with efficient disclose of attributes

Main steps

$$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}=\text{"18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$$

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(\vec{m}) + \vec{m}$

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(\vec{m}) + \vec{m}$

  provides $\longrightarrow$ Integrity of $\vec{m}$

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(\vec{m}) + \vec{m}$

  provides $\longrightarrow$ Integrity of $\vec{m}$

- Π=Proof of ownership of σ on $\vec{m}' = (m_{i_1}, \ldots, m_{i_\ell})$ s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, \vec{m}')$

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}=\texttt{"18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(\vec{m}) + \vec{m}$

  provides $\longrightarrow$ Integrity of $\vec{m}$

- Π=Proof of ownership of σ on $\vec{m}' = (m_{i_1}, \ldots, m_{i_\ell})$ s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, \vec{m}')$

  provides $\longrightarrow$ Rightness of id

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(\vec{m}) + \vec{m}$

  provides $\longrightarrow$ Integrity of $\vec{m}$

- Π=Proof of ownership of σ on $\vec{m}' = (m_{i_1}, \ldots, m_{i_\ell})$ s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, \vec{m}')$

  provides $\longrightarrow$ Rightness of id

- Proof of ownership of σ s.t.
  $\text{Verify}(\text{pk}_{\text{id}}, \sigma, \vec{m}')$ + **without revealing** $\vec{m}'$
  and $\mathcal{R}(\vec{m}', \vec{X})$ where $\vec{X}$ contains public attributes

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(\vec{m}) + \vec{m}$

  provides $\longrightarrow$ Integrity of $\vec{m}$

- Π=Proof of ownership of σ on $\vec{m}' = (m_{i_1}, \ldots, m_{i_\ell})$ s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, \vec{m}')$

  provides $\longrightarrow$ Rightness of id

- Proof of ownership of σ s.t.
  $\text{Verify}(\text{pk}_{\text{id}}, \sigma, \vec{m}')$ + **without revealing** $\vec{m}'$
  and $\mathcal{R}(\vec{m}', \vec{X})$ where $\vec{X}$ contains public attributes

Main steps

$\texttt{Valid}(\text{passeport}_{\text{id}}) \wedge \text{Age}_{\text{id}}\texttt{="18"} \wedge \texttt{Valid}(\text{credit card}_{\text{id}}) \wedge \texttt{SameId}$

- $\text{Sign}(\vec{m}) + \vec{m}$

  provides $\longrightarrow$ Integrity of $\vec{m}$

- Π=Proof of ownership of σ on $\vec{m}' = (m_{i_1}, \ldots, m_{i_\ell})$ s.t.$\text{Verify}(\text{pk}_{\text{id}}, \sigma, \vec{m}')$

  provides $\longrightarrow$ Rightness of id

- Proof of ownership of σ s.t.
  $\text{Verify}(\text{pk}_{\text{id}}, \sigma, \vec{m}')$ + **without revealing** $\vec{m}'$
  and $\mathcal{R}(\vec{m}', \vec{X})$ where $\vec{X}$ contains public attributes

  provides $\longrightarrow$ Anonymous Authentication of pk_{id}

Syntactical Definition of Bw-Psigs (1/2)

Syntactical Definition of Bw-Psigs (1/2)

- Setup(λ): generates params

Syntactical Definition of Bw-Psigs (1/2)

- Setup(λ): generates params
- SigSetup(params): outputs pk, sk

Syntactical Definition of Bw-Psigs (1/2)

- Setup(λ): generates params
- SigSetup(params): outputs pk, sk
- Sign(sk, $\vec{m}$): outputs σ
  (whose size is independent of $|m|$)

Syntactical Definition of Bw-Psigs (1/2)

- Setup(λ): generates params
- SigSetup(params): outputs pk, sk
- Sign(sk, $\vec{m}$): outputs σ
  (whose size is independent of $|m|$)
- Verify(pk, $\vec{m}, \sigma$): outputs 1 or 0

Syntactical Definition of Bw-Psigs (1/2)

- Setup(λ): generates params
- SigSetup(params): outputs pk, sk
- Sign(sk, $\vec{m}$): outputs σ
  (whose size is independent of $|m|$)
- Verify(pk, $\vec{m}, \sigma$): outputs 1 or 0
- WitGen(pk, $R, i, m, \vec{X}, \sigma$): computes a witness W_i proving that σ is a signature on some $\vec{m}$ such that:

$$(1) \quad \vec{m}_i = m \quad \text{and} \quad (2) \quad R(i, \vec{m}, \vec{X}) = 1$$

Syntactical Definition of Bw-Psigs (1/2)

- Setup(λ): generates params
- SigSetup(params): outputs pk, sk
- Sign(sk, $\vec{m}$): outputs σ
  (whose size is independent of $|m|$)
- Verify(pk, $\vec{m}, \sigma$): outputs 1 or 0
- WitGen(pk, $R, i, m, \vec{X}, \sigma$): computes a witness W_i proving that σ is a signature on some $\vec{m}$ such that:

$$(1) \quad \vec{m}_i = m \quad \text{and} \quad (2) \quad R(i, \vec{m}, \vec{X}) = 1$$

- WitVerify(pk, $R, i, \vec{X}, W, \sigma$): outputs 1 if W gives evidence that σ is valid for some $\vec{m}$ such that (1) and (2) hold

Syntactical Definition of Bw-Psigs (2/2)

- SigProve(pk, $R, i, \sigma, \vec{m}, \vec{X}$): generates a proof of the knowledge of some W such that Verify(pk, $\vec{m}, \sigma$) $= 1$ for and WitVerify(pk, $R, i, \vec{X}, W, \sigma$) $= 1$
- the corresponding ProofVerify algorithm

Syntactical Definition of Bw-Psigs (2/2)

- SigProve(pk, $R, i, \sigma, \vec{m}, \vec{X}$): generates a proof of the knowledge of some W such that Verify(pk, $\vec{m}, \sigma$) $= 1$ for and WitVerify(pk, $R, i, \vec{X}, W, \sigma$) $= 1$
- the corresponding ProofVerify algorithm
- SigIssue(sk, C_{m_1}, m_2) $\leftrightarrow$ SigObtain(pk, $m_2, open_{m_1}$), where $\vec{m} = m_1|m_2$: allows $\mathcal{U}$ to obtain a signature on a partial commitment C_{m_1} without letting know m_1

Issuing $cred$ anonymously

- CredSetup(params): runs Setup(λ)
- OKeygen(params): runs SigSetup(λ)
- UKeygen(params): picks $\mathsf{sk}_{\mathcal{U}}$ and computes $\mathsf{pk}_{\mathcal{U}}$

User $(\mathsf{sk}_{\mathcal{U}}, \mathsf{pk}_{\mathcal{U}})$

$N_1 = \mathsf{Com}(\mathsf{sk}_{\mathcal{U}}, open_{\mathcal{U}}) + \Pi_{\mathcal{U}}$

$\vec{m} = m_1 | m_2, \Pi_1$

$C_1 = \mathsf{VecCom}(\mathsf{sk}_{\mathcal{U}} | m_1, open_{m_1})$

$cred$

$\xrightarrow{N_1, \Pi_{\mathcal{U}}}$

$\xrightarrow{C_1, \Pi_1, m_2}$

SigObtain,SigIssue $\leftrightarrow$

Org$_1$ $(\mathsf{pk}_1, \mathsf{sk}_1)$

$\mathsf{ProofVerify}(\Pi_1)$
$\mathsf{ProofVerify}(\Pi_{\mathcal{U}})$

NI Proof for $cred$

1. User $(N_2, aux, \mathsf{sk}_{\mathcal{U}}, cred, R, i, \vec{m}, \vec{X})$

   Parse $cred$ as a Bw-Psigs

   $\Pi_{\mathcal{U}} = \mathsf{SigProve}(\mathsf{pk}_{\mathcal{U}}, R^{=}, 1, \sigma, \vec{m}, (\mathsf{sk}_{\mathcal{U}}, 0, \ldots, 0))$

   $\Pi_2 = \mathsf{SigProve}(\mathsf{pk}_{\mathcal{U}}, R, i, \sigma, \vec{m}, \vec{X})$ and sends $\Pi_{\mathcal{U}}, \Pi_2$ to Org_2

2. $\mathsf{Org}_2(N_2, i, R, \Pi_{\mathcal{U}}, \Pi_2)$

   $\mathsf{ProofVerify}(\mathsf{pk}, R^{=}, 1, \Pi_{\mathcal{U}}) \stackrel{?}{=} \mathsf{ProofVerify}(\mathsf{pk}, R, i, \Pi_2, \vec{X}) \stackrel{?}{=} 1$

Main Ingredient

A compact and functional commitment scheme

Public $(g, g_1, \ldots, g_{2n})$, s.t. $g_i = g^{a^i}$, $a \xleftarrow{\mathcal{R}} \mathbb{Z}_p$,

- Commitment of $\vec{m} \rightsquigarrow C = g^r \prod_{j=1}^{n} g_{n+1-j}^{m_j}$

Main Ingredient

A compact and functional commitment scheme

Public $(g, g_1, \ldots, g_{2n})$, s.t. $g_i = g^{a^i}$, $a \xleftarrow{\mathcal{R}} \mathbb{Z}_p$,

- Commitment of $\vec{m} \rightsquigarrow C = g^r \prod_{j=1}^{n} g_{n+1-j}^{m_j}$
- Witness for $m_i \rightsquigarrow W_i = g_i^r \cdot \prod_{j=1, j\neq i}^{n} g_{n+1-j+i}^{m_j}$ satisfies

$$e(g_i, C) = e(g_1, g_n)^{m_i} \cdot e(g, W_i)$$

Main Ingredient

A compact and functional commitment scheme

Public $(g, g_1, \ldots, g_{2n})$, s.t. $g_i = g^{a^i}$, $a \xleftarrow{\mathcal{R}} \mathbb{Z}_p$,

- Commitment of $\vec{m} \rightsquigarrow C = g^r \prod_{j=1}^{n} g_{n+1-j}^{m_j}$
- Witness for $m_i \rightsquigarrow W_i = g_i^r \cdot \prod_{j=1, j\neq i}^{n} g_{n+1-j+i}^{m_j}$ satisfies

$$e(g_i, C) = e(g_1, g_n)^{m_i} \cdot e(g, W_i)$$

- To convince that $\mathcal{S} : \vec{X} \cdot \vec{m} = 0$

Main Ingredient

A compact and functional commitment scheme

Public $(g, g_1, \ldots, g_{2n})$, s.t. $g_i = g^{a^i}$, $a \xleftarrow{\mathcal{R}} \mathbb{Z}_p$,

- Commitment of $\vec{m} \rightsquigarrow C = g^r \prod_{j=1}^{n} g_{n+1-j}^{m_j}$
- Witness for $m_i \rightsquigarrow W_i = g_i^r \cdot \prod_{j=1, j\neq i}^{n} g_{n+1-j+i}^{m_j}$ satisfies

$$e(g_i, C) = e(g_1, g_n)^{m_i} \cdot e(g, W_i)$$

- To convince that $\mathcal{S} : \vec{X} \cdot \vec{m} = 0$
  1. $\mathcal{P}$ computes $W = \prod_i W_i$ to $\mathcal{V}$

Main Ingredient

A compact and functional commitment scheme

Public $(g, g_1, \ldots, g_{2n})$, s.t. $g_i = g^{a^i}$, $a \xleftarrow{\mathcal{R}} \mathbb{Z}_p$,

- Commitment of $\vec{m} \rightsquigarrow C = g^r \prod_{j=1}^{n} g_{n+1-j}^{m_j}$
- Witness for $m_i \rightsquigarrow W_i = g_i^r \cdot \prod_{j=1, j\neq i}^{n} g_{n+1-j+i}^{m_j}$ satisfies

$$e(g_i, C) = e(g_1, g_n)^{m_i} \cdot e(g, W_i)$$

- To convince that $\mathcal{S} : \vec{X} \cdot \vec{m} = 0$
  1. $\mathcal{P}$ computes $W = \prod_i W_i$ to $\mathcal{V}$
  2. $\mathcal{V}$ verifies $e(\prod_{i=1}^{n} g_i^{x_i}, C) \stackrel{?}{=} e(g, \prod_{i=1}^{n} W)$

Main Ingredient

A compact and functional commitment scheme

Public $(g, g_1, \ldots, g_{2n})$, s.t. $g_i = g^{a^i}$, $a \xleftarrow{\mathcal{R}} \mathbb{Z}_p$,

- Commitment of $\vec{m} \rightsquigarrow C = g^r \prod_{j=1}^{n} g_{n+1-j}^{m_j}$
- Witness for $m_i \rightsquigarrow W_i = g_i^r \cdot \prod_{j=1, j\neq i}^{n} g_{n+1-j+i}^{m_j}$ satisfies

$$e(g_i, C) = e(g_1, g_n)^{m_i} \cdot e(g, W_i)$$

- To convince that $\mathcal{S} : \vec{X} \cdot \vec{m} = 0$
  1. $\mathcal{P}$ computes $W = \prod_i W_i$ to $\mathcal{V}$
  2. $\mathcal{V}$ verifies $e(\prod_{i=1}^{n} g_i^{x_i}, C) \stackrel{?}{=} e(g, \prod_{i=1}^{n} W)$
- Similar for $\vec{m} \cdot \vec{X} \neq 0$

Handled predicates with IP

As [KSW08], define

$$R^{\text{poly}}(f, w) = 1 \text{ iff } f(w) = 0, \text{ where } f(Z) = \sum_{i=1}^{n} \rho_i Z$$

$$\vec{m} = (\rho_0, \ldots, \rho_{n-1}) \text{ and } \vec{X} = (1, w, w^2, \ldots, w^{n-1})$$

Predicate	Implementation as a polynomial
$(z = I_1) \vee (z = I_2) \cdots \vee (z = I_{n-1})$	$f_{\text{OR},\vec{I}}(z) = \prod_{j=1}^{n-1}(z - I_j) = 0$
$(z_1 = I_1) \vee (z_2 = I_2) \vee \cdots \vee (z_{n-1} = I_{n-1})$	$f_{\overline{\text{OR}},\vec{I}}(\vec{z}) = \prod_{j=1}^{n-1}(z_j - I_j) = 0$
$(z_1 = I_1) \wedge (z_2 = I_2) \cdots \wedge (z_{n-1} = I_{n-1})$	$f_{\text{AND},\vec{I}}(\vec{z}) = \sum_{j=1}^{n-1} r_j(z_j - I_j) = 0$
$(z_1 \neq I_1) \vee (z_2 \neq I_2) \cdots \vee (z_{n-1} \neq I_{n-1})$	$f_{\text{OR-NOT},\vec{I}}(\vec{z}) = \sum_{j=1}^{n-1} r_j(z_j - I_j) \neq 0$
$(z \neq I_1) \wedge (z \neq I_2) \wedge \cdots \wedge (z_{n-1} \neq I_{n-1})$	$f_{\text{AND-NOT},\vec{I}}(z) = \prod_{j=1}^{n-1}(z - I_j) \neq 0$
$(z_1 \neq I_1) \wedge (z_2 \neq I_2) \wedge \cdots \wedge (z_{n-1} \neq I_{n-1})$	$f_{\overline{\text{AND-NOT}},\vec{I}}(\vec{z}) = \prod_{j=1}^{n-1}(z_j - I_j) \neq 0$

Extension to inexact threshold

Efficiency

	Size	Generation	Verification Batch
Algorithm $\mathsf{SigProve}_1$			
$R = R^{\mathsf{EQ}}$	80	$80 \cdot$ MultiExp	$18 \cdot$ Pairings
$R = R^{\neg\mathsf{EQ}}$	101	$101 \cdot$ MultiExp	$20 \cdot$ Pairings
Algorithm $\mathsf{SigProve}_2$			
$R = R^{\mathsf{IP}}$	65	$66 \cdot$ MultiExp	$15 \cdot$ Pairings
$R = R^{\neg\mathsf{IP}}$	104	$105 \cdot$ MultiExp	$20 \cdot$ Pairings
$R = R^{\mathsf{EQ}}$	77	$77 \cdot$ MultiExp	$16 \cdot$ Pairings
$R = R^{\neg\mathsf{EQ}}$	107	$107 \cdot$ MultiExp	$20 \cdot$ Pairing

Conclusion

- Minimize the number of interaction
- Extend P-signature $\longrightarrow$ Block-wise P-signature (Bw-Psigs)

  A more general class of predicates *via* inner product
- **Application: Non-interactive Anonymous Credentials with efficient disclosure of attributes**