PS signatures

Key generation

- Pick generator $\tilde{g} \in_R G_2$
- Private key: $(x, y_1, \ldots, y_L) \in_R \mathbb{Z}_p$
- Public key:
  $(\tilde{g}, \tilde{X}, \tilde{Y_1}, \ldots, \tilde{Y_L}) = (\tilde{g}, \tilde{g}^x, \tilde{g}^{y_1}, \ldots, \tilde{g}^{y_L})$

Signing tuple $(m_1, \ldots, m_L)$

- Pick $h \in_R G_1^*$ and output
- Signature $\sigma = \left(h, h^{x+\sum y_i m_i}\right)$

Part of "Secret Stroll" project

Cryptography sidebar

Cyclic groups: G_1, G_2, G_T
Generators: $g, \tilde{g}, g_T$
Group order: p

Pairing: $e : G_1 \times G_2 \rightarrow G_T$
Bilinear: $e(g^a, \tilde{g}^b) =$

Verifying a signature:

- Given a signature $\sigma = (\sigma_1, \sigma_2)$
- Message: $(m_1, \ldots, m_L)$
- And public key $(\tilde{g}, \tilde{X}, \tilde{Y_1}, \ldots, \tilde{Y_L})$
- Check:
  - $\sigma_1 \neq 1_{G_1}$
  - $e\left(\sigma_1, \tilde{X} \cdot \prod \tilde{Y_i}^{m_i}\right) = \mathrm{e}(\sigma_2, \tilde{g})$

Issuing a PS credential

- User commits to hidden attributes, pick $t \in_R \mathbb{Z}$

$$C = g^t \prod_{i \in U} Y_i^{a_i}$$

- And proves that she did so correctly:

$$PK\left\{(t, (a_i)_{i \in U}) : C = g^t \prod_{i \in U} Y_i^{a_i}\right\}$$

- Issuer verifies the proof, picks $u \in_R \mathbb{Z}_p$ and sets:

$$\sigma' = \left(g^u, \left(XC \prod_{i \in I} Y_i^{a_i}\right)^u\right)$$

- User forms signature $\sigma = (\sigma_1', \frac{\sigma_2'}{\sigma_1'^t})$

Proof shows that *C* is correctly formed. What goes wrong if you omit this?

Attribute sets:
U: attributes **determined by user** (hidden from issuer)
I: attributes **determined by issuer**

Cryptography sidebar

Cyclic groups: G_1, G_2, G_T
Generators: $g, \tilde{g}, g_T$
Group order: p

Pairing: $e : G_1 \times G_2 \rightarrow G_T$
Bilinear: $e(g^a, \tilde{g}^b) = e(g, \tilde{g})^{ab}$

PS Signatures
Private key: $(x, y_1, \ldots, y_L) \in_R \mathbb{Z}_p$ and $X = g^x$
Public key:
$(\tilde{g}, \tilde{X}, \tilde{Y}_i) = (\tilde{g}, \tilde{g}^x, \tilde{g}^{y_i}) \in G_2$ **and** $(g, Y_i) = (g, g^{y_i}) \in G_1$

Signature: $\sigma = (\sigma_1, \sigma_2)$ such that $\sigma = (h, h^{x + \sum y_i m_i}) \in G_1^2$

Extra parts of pk

Proving possession of a credential

- User has a credential $\sigma = (\sigma_1, \sigma_2)$ on $(a_1, \dots, a_L)$
- Pick $r, t \in_R \mathbb{Z}_p$ and compute $\sigma' = (\sigma_1^r, (\sigma_2 \sigma_1^t)^r)$
- Send σ' and disclosed attributes $(a_i)_{i \in D}$
- And proves that the signature is valid:

$$PK\left\{(t, (a_i)_{i\in H}): \frac{e(\sigma_2', \tilde{g})\prod_{i\in D} e\left(\sigma_1', \tilde{Y}_j\right)^{-a_i}}{e\left(\sigma_1', \tilde{X}\right)} = e(\sigma_1', \tilde{g})^t \prod_{i\in H} e\left(\sigma_1', \tilde{Y}_i\right)^{a_i}\right\}$$

- The verifier accepts if proof is valid and $\sigma_1' \neq 1$

What goes wrong if you omit this?

Attribute sets:
H: hidden attributes
D: disclosed attributes
Different from previous slide!!!

$$e\left(\sigma_1', \tilde{g}^t \tilde{X} \cdot \prod \tilde{Y}_i^{a_i}\right) = e(\sigma_2', \tilde{g})$$

Cryptography sidebar

Cyclic groups: G_1, G_2, G_T
Generators: g, h, g_T
Group order: p

Pairing: $e : G_1 \times G_2 \rightarrow G_T$
Bilinear: $e\left(g^a, h^b\right) = e(g, h)^{ab}$

PS Signatures
Private key: $(x, y_1, \dots, y_L) \in_R \mathbb{Z}_p\ \mathbb{Z}_p$ and $X = g^x$
Public key:
$(g, Y_i) = (g, g^x, g^{y_i}) \in G_1$
$\left(\tilde{g}, \tilde{X}, \tilde{Y}_i\right) = (\tilde{g}, \tilde{g}^x, \tilde{g}^{y_i}) \in G_2$

Signature: $\sigma = (\sigma_1, \sigma_2)$ such that
$\sigma = \left(h, h^{x+\sum y_i a_i}\right) \in G_1^2$