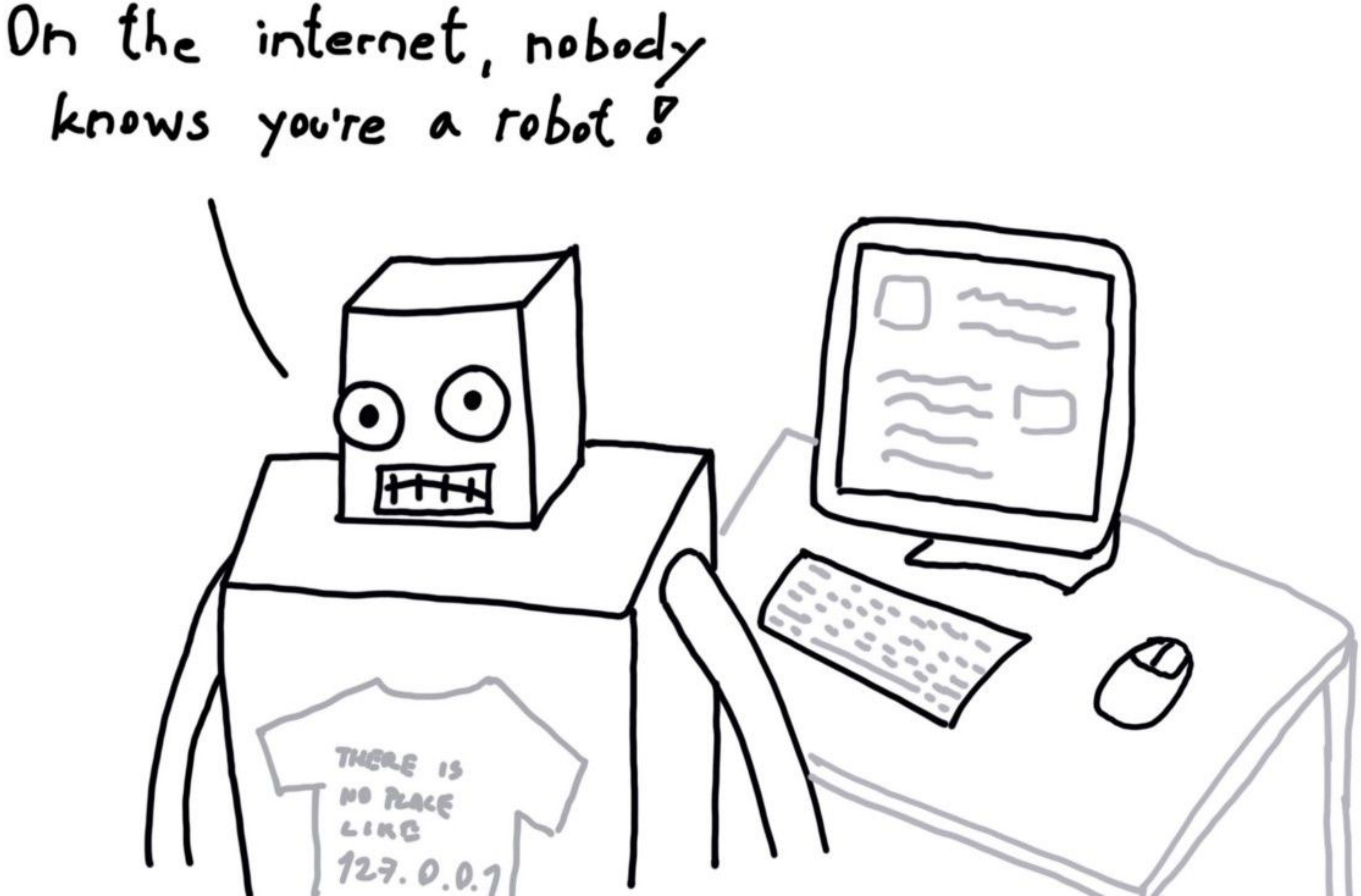
Ockam Credentials

Pairing-Based Cryptography + Short Group Signatures = Secure & Private Credentials for IoT


On the internet, nobody knows you're a robot!
THERE IS NO PLACE LIKE 127.0.0.1

Enter Ockam Credentials

- Multi Message Digital Signatures
- Allows claims to be shown or withheld
- Never present actual signature
- Instead, send proof of validity

Recommended solution	Short Group Signatures for initial login, Privacy Pass afterwards						
Properties	Username & Password	Token	Signatures	Privacy Pass	SSO (Active Directory, LDAP, X.500) OpenID connect, OAuth	PKI	Short Group Signatures (CL, BBS+,
Presenter ID	yes	no	yes	no	yes	yes	yes
Signer ID	no	no	no	yes	yes	yes	yes
Revocation	no	no	no	no	yes	yes	yes
Internal	yes	yes	yes	yes	no	no	yes
Portable	yes	no	yes	no	yes	yes	yes
Complexity (1-5)	1	2	2	3	4	4	5
Size (1-5)	2	2	1	1	5	3	5
Computation Load (1-5)	5	1	1	2	4	1	4
Privacy (1-5)	5	3	3	1	3	5	1
Information (1-5)	4	1	1	1	4	5	1
Implementation (1-5)	5	3	1	2	4	1	5
Reversible (1-5)	4	3	3	1	2	3	1

Group Signatures

- Designed for multiple signers
- Single public key
- Signer anonymity
- Group manager can remove anonymity

Short group signatures

- Group manager is issuer
- Use signer key as credential
- Signature over multiple messages
- Allows Proofs of Knowledge of Signatures vs Disclosing signature
- Allows selective disclosure of signed messages
- Relies on Pairings

Math Intro Elliptic Curves

- A new operation called *pairing*
- Curves support it – Pairing friendly
- Pairing friendly curves have two fields vs one
    - Denoted as G_1 and G_2
- Denoted with e
- Mathematically works like

$$e(sH_0, m_1H_1) == e(H_0, H_1)^{sm_1}$$
$$e(sm_1H_0, H_1) == e(H_0, H_1)^{sm_1}$$
$$e(H_0, sm_1H_1) == e(H_0, H_1)^{sm_1}$$

- Used in verification albeit slower
- Called *Bilinear Maps*

Real World

- Boneh, Boyen, Shachum (BBS+)
  - Signature = 1 Group 1 element, 2 Field elements
  - Public key = Group 1 element per message + 1 extra Group 1 for blinding, 1 Group 2 element
  - Secret key = 1 Field element
- Pointcheval Saunders (PS)
  - Signature = 2 Group 1 elements
  - Public key = Group 2 elements per message + 1 extra Group 2 for blinding
  - Secret key = Field element per message + 1 extra field element
- Both can work with thresholds
  - PS is easier to do this

Setup

- Pairing friendly curve
- $P \in \mathbb{G}_1$
- $\widetilde{P} \in \mathbb{G}_2$
- p is base point order
- e is pairing function

BBS+

- Secret key $\alpha \xleftarrow{\$} p$
- Public Key $\widetilde{Q} = \alpha\widetilde{P}$
  - $H_i = H_{\mathbb{G}_1}(\widetilde{Q}, i, 0, len(messages))$

BBS+

- $\sigma = Sign(\alpha, \{m_1, \ldots, m_N\})$
- Generate H's, random s, e < *p*
- Compute

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha+e}}$$

- $\sigma = \{A, e, s\}$

BBS+

- Holder
  - Generate random s’
  - Compute $U = H_0^{s'} H_1^{m_1}$
  - Send U to issuer
- Issuer
  - Generate s’’, e
  - Compute
  - $$S = UH_0^{s''} \sum_{i=2}^{N} H_i^{m_i}$$

    $$A = S^{\frac{1}{\alpha+e}}$$
- Holder
  - Compute s = s’ + s’’
  - $$\sigma = \{A, e, s\}$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha+e}}$$

$$\widetilde{Q} = \alpha\widetilde{P}$$

$$e(A, \widetilde{Q} + e\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha+e}}$$

$$\widetilde{Q} = \alpha\widetilde{P}$$

$$e(A, \widetilde{Q} + e\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

$$e(A, \widetilde{Q} + e\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha+e}}$$

$$\widetilde{Q} = \alpha\widetilde{P}$$

$$e(A, \widetilde{Q} + e\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

$$e(A, \alpha\widetilde{P} + e\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha + e}}$$

$$\widetilde{Q} = \alpha \widetilde{P}$$

$$e(A, \alpha\widetilde{P} + e\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

$$e(A, \alpha\widetilde{P} + e\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha+e}}$$

$$\widetilde{Q} = \alpha\widetilde{P}$$

$$e(A, \alpha\widetilde{P} + e\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

$$e(A, (\alpha + e)\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha+e}}$$

$$\widetilde{Q} = \alpha \widetilde{P}$$

$$e(A, (\alpha + e)\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

$$e(A, (\alpha + e)\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha+e}}$$

$$\widetilde{Q} = \alpha\widetilde{P}$$

$$e(A, (\alpha + e)\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

$$e(S^{\frac{1}{\alpha+e}}, (\alpha + e)\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$
$$A = S^{\frac{1}{\alpha+e}}$$
$$\widetilde{Q} = \alpha\widetilde{P}$$

$$e(S^{\frac{1}{\alpha+e}}, (\alpha + e)\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$
$$e(S^{\frac{1}{\alpha+e}}, (\alpha + e)\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha+e}}$$

$$\widetilde{Q} = \alpha \widetilde{P}$$

$$e(S^{\frac{1}{\alpha+e}}, (\alpha + e)\widetilde{P}) \stackrel{?}{=} e(S, \widetilde{P})$$

$$e(S, \widetilde{P})^{\frac{\alpha+e}{\alpha+e}} \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- $Verify(\widetilde{Q}, \sigma, \{m_1, \ldots, m_N\})$

$$S = H_0^s \sum_{i=1}^{N} H_i^{m_i}$$

$$A = S^{\frac{1}{\alpha+e}}$$

$$\widetilde{Q} = \alpha\widetilde{P}$$

$$e(S, \widetilde{P})^{\frac{\alpha+e}{\alpha+e}} \stackrel{?}{=} e(S, \widetilde{P})$$

$$e(S, \widetilde{P})^{1} \stackrel{?}{=} e(S, \widetilde{P})$$

BBS+

- Prove({m}, {A, e, s}) = Π

$$r_1, r_2, \widetilde{r_2}, \widetilde{x}, \widetilde{e} \xleftarrow{\$} p \qquad \widetilde{m}_{i \in A_H} \xleftarrow{\$} p$$

$$r_3 = r_1^{-1} \mod p \qquad S = sH_0 \sum_{i=1}^{N} m_i H_i \quad A' = r_1 A$$

$$\overline{A} = r_1 S - eA'$$

$$D = r_1 S - r_2 H_0 \qquad x = s - r_2 r_3 \qquad T_1 = \widetilde{r_2} H_0 - \widetilde{e} A'$$

$$T_2 = \widetilde{r_3} D - \widetilde{x} H_0 \sum_{i=1}^{A_H} \widetilde{m_i} H_i \qquad R = P \sum_{i=1}^{A_D} m_i H_i \qquad c = \mathcal{H}(A', \overline{A}, D, R, T_1, T_2)$$

$$\widehat{e} = \widetilde{e} - ce \qquad \widehat{r_2} = \widetilde{r_2} - cr_2 \qquad \widehat{r_3} = \widetilde{r_3} - cr_3$$

$$\widehat{x} = \widetilde{x} - cx \qquad \widehat{m_i} = \widetilde{m_i} - cm_i$$

BBS+

- Verify(Π, {m} in A_D)
- Check $A' \neq 1$
- $$T_1 = c(\overline{A} - D) - \widehat{e}A'\widehat{r_2}H_0$$
  $$T_2 = cR + \widehat{r_3}D - \widehat{x}H_0 - \left(\sum_{i+1}^{A_H} \widehat{m_i}H_i\right)$$
  $$c \stackrel{?}{=} \mathcal{H}(A', \overline{A}, D, R, T_1, T_2)$$

Credential Cryptography

- Short group signatures
  - Selective disclosure and proof of validity
- BLS signatures
  - Small, Aggregate, Threshold
- Accumulators
  - Anonymous set membership (check if value is in a set with disclosing the value)
- Verifiable Oblivious Pseudorandom Functions (VOPRF)
  - Anonymous or blinded tokens

Use cases

- Enrollment
- Authentication
- Authorization