Dynamic Attribute Serialization for performance improvement in anonymous credential system

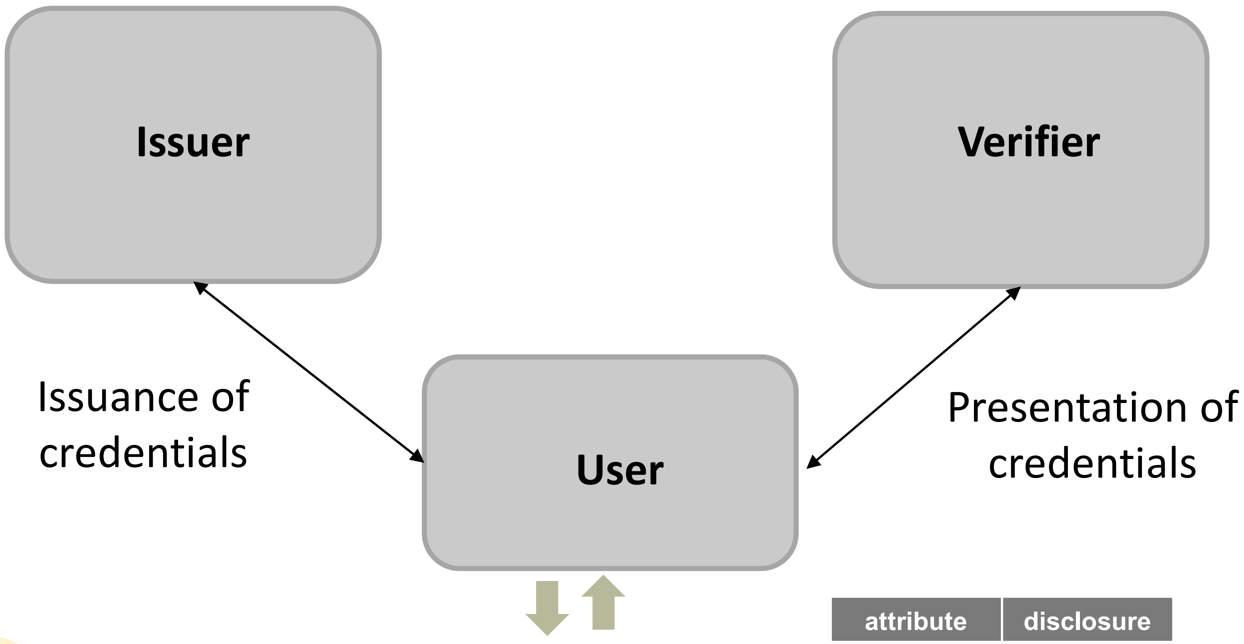
02123014 장지운

2023.12.07

EZID

- Attribute-based credentials
  - ✓ selective disclosure of attributes
- Auditability
- Revocation

EZID: Three Basic Components



Verifiable Credential

Data Storage

Digital Wallet

attribute	disclosure
0	X
1	X
2	O (>18)
3	X

Selective Disclosure

EZID Protocol: Overview

Preprocessing Process

- **Attribute (Format) Definition**
- **- SetUp**
  - Key Generation

VC Issuance

Credential Request

- **Attribute Value Definition**

a_0	a_1	a_2	…	a_n
User Private Key	Att1	Att2		Att4

- **Commitment Computation**
- **(opt) Proof Generation for Commitment**

Credential Issuance

- **Issuer Signature for Commitment, σ Generation**
- **Private Key Setup/Storage:** $(\sigma, a_0 = x, a_1 \ldots, a_n)$
- **Private Key Storage Delegation Server**

VC Presentation

Credential Presentation

- **Selective Exposure Definition**

a_0	a_1	a_2	…	a_n

e.g., a2>19
Determination of Attributes to be Disclosed or Attributes' Function

- **Proof of Possession Value Generation by the Issuer Based on Selective Exposure**

Credential Verification

- **Verification of Issuer's Signature, Proof of Possession Value, and Selective Exposure**

EZID Protocol: Types of Attributes

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}

	Attribute Name		Explanation
A0	Secret Key	λ_0-bit Sequence	Random Sequence, e.g., λ=128
A1	Name		Hong Gil-dong
A2	Date of Birth	8-digit Decimal	e.g., 20000101
A3	Gender	Bit	1(Female) or 2(Male)
A4	Address	Postal Code, 5-digit Decimal	e.g., 34129
A5		City, Postal Code	Daejeon
A6		Detailed Address, λ_6-bit String	218, Gajeong-ro, Yuseong-gu, ETRI Information Security Research Division

	Attribute Name		Explanation
A7	Mobile Phone Number	11-digit Decimal	e.g., 11112341234
A8	CARD Information	Issuer λ_8-bit String	BC
A9		Number, 16-digit Decimal	1234-5678-9012-3456
A10		Expiration Date, 8-digit Decimal	20211231

EZID Protocol: Basic Operations

- Bilinear map and Group, $e: G_1 \times G_2 \rightarrow G_T$: a Type III pairing
  - where G_1, G_2, G_T have the order of prime q
- Pedersen Commitment

$$f(a_0, \ldots, a_n) = \prod_{i=0}^{n} u_i^{a_i} = u_0^{a_0} u_1^{a_1} \cdots u_n^{a_n}$$

Secret Key

Attribute Value

- Issuer's signature: BBS+ signature for attributes $(a_0 = x, a_1 \ldots, a_n)$

$$A = \left(g_1 g_2^{y} u_0^{a_0} \prod_{i=1}^{n} u_i^{a_i} \right)^{\frac{1}{\theta + \mu}} \qquad \sigma = (A, \mu, y), \qquad A \in G_1, \mu, y \in \mathbb{Z}_q$$

- SPK $(y', a_0, a_1, \ldots, a_n) : F = g_2^{y'} \prod_{i=0}^{n} u_i^{a_i}$ for a possession of a BBS+ signature

Dynamic Attribute Serialization(DAS) Overview

- ❖ Purpose
  - ✓ When using anonymous credentials, reduce computational complexity during signature and verification to improve performance
- ❖ Method
  1. Generate transformed values for attributes (a'_i) to store the transformed attribute values (a_i)
  2. Define $\overline{D}$ as the indices of attributes for which "selective disclosure" is not performed
  3. Define $\bar{i} = MIN(\overline{D})$ as the smallest index value among $\overline{D}$
  4. Execute concatenation and hash operations on all attributes not subject to "selective disclosure" ($a_{\forall i \in \overline{D}}$) and store the result in the attribute with the smallest index ($a'_{\bar{i}}$)
  5. Set the values of the remaining attributes ($a'_{\forall i \in \overline{D}} \backslash a'_{\bar{i}}$) to '0' for attributes not subject to "selective disclosure" ($a_{\forall i \in \overline{D}}$)
     - Since $a'_i = 0$ in the multiplication of attributes ($u_i^{a'_i}$), $u_i^0 = 1$ for all attributes.
  6. For attributes subject to "selective disclosure" ($a_{\forall i \in DI}$), store each $a_{i \in DI}$ value in the corresponding attribute $a'_{i \in DI}$

DAS Overview (cont.)

❖ Example

- ✓ Assume that $n = 6$, $\mathrm{DI} = \{1, 3, 5\}$, $\overline{D} = \{2, 4, 6\}$
- ✓ $MIN(\overline{D}) = \bar{i} = 2$
- ✓ $a'_{\bar{i}} = a'_2 = \mathrm{Hash}(a_2||a_4||a_6)$ $(\because a'_{\bar{i}} = \mathrm{Hash}(||a_{\forall i \in \overline{D}}))$
- ✓ $a'_4 = 0,\ a'_6 = 0$ $(\because a'_{\forall i \in \overline{D}} \backslash a'_{MIN(\overline{D})} = 0)$
- ✓ $a'_1 = a_1,\ a'_3 = a_3,\ a'_5 = a_5$ $(\because a'_{i \in DI} = a_{i \in DI})$
- ✓ $\prod_{i=0}^{n} u_i^{a'_i} = u_0^{a_0} u_1^{a'_1} u_2^{a'_2} u_3^{a'_3} u_4^{a'_4} u_5^{a'_5} u_6^{a'_6} = u_0^{a_0} u_1^{a_1} u_2^{\mathrm{Hash}(a_2||a_4||a_6)} u_3^{a_3} u_4^{0} u_5^{a_5} u_6^{0} = u_0^{a_0} u_1^{a_1} u_2^{\mathrm{Hash}(a_2||a_4||a_6)} u_3^{a_3} u_5^{a_5}$

EZID Protocol: Presentation

- R_2

$$
\begin{aligned}
&= e(D_2,h)^{s_\mu} e(u_0,h_\theta)^{s_\alpha} e(u_0,h)^{s_\gamma} e(g_2,h)^{s_y} \prod_{i\in\overline{D}} e(u_i,h)^{s_i} \cdot \left(e(D_2,h_\theta)\left(\prod_{i\in \mathrm{DI}} e(u_i,h)^{-s_i}\right) e(g_1,h)^{-1}\right)^{c} \\
&= e(D_2,h^{s_\mu} h_\theta^{c}) e(u_0,h_\theta)^{r_\alpha - c\cdot\alpha} e(u_0,h)^{r_\gamma - c\cdot\gamma} e\left(g_1^{-c} g_2^{r_y - c\cdot y} \prod_{i\in\overline{D}} u_i^{r_i - c\cdot a_i}, h\right) \left(e\left(\prod_{i\in \mathrm{DI}} u_i^{-c\cdot a_i} u_i, h\right)\right. \\
&= e(D_2,h^{r_\mu + c\cdot\mu} h_\theta^{c}) e\left(u_0,h^{\theta}\right)^{-c\cdot\alpha} e(u_0,h)^{-c\cdot(\alpha\mu+z)} e\left(g_1^{-c} g_2^{-c\cdot y} \prod_{i=1}^{n} u_i^{-c\cdot a_i}, h\right) e(u_0,h_\theta)^{r_\alpha} e\left(g_2^{r_y} u_0^{r_\gamma} \prod_{i\in\overline{D}} u_i^{r_i}, h\right) \\
&= e\left(D_2, h^{r_\mu} h^{(\theta+\mu)c}\right) e(u_0,h)^{-c(\alpha\theta+\alpha\mu+z)} e\left(g_1^{-c} g_2^{-c\cdot y} \prod_{i=1}^{n} u_i^{-c\cdot a_i}, h\right) e\left(u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} \prod_{i\in\overline{D}} u_i^{r_i}, h\right) \\
&= e\left(A\cdot u_0^{\alpha}, h^{(\theta+\mu)c}\right) e(u_0,h)^{-c\alpha(\theta+\mu)} e(u_0,h)^{-c a_0} e\left(g_1^{-c} g_2^{-c\cdot y} \prod_{i=1}^{n} u_i^{-c\cdot a_i}, h\right) e\left(D_2^{r_\mu} u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} \prod_{i\in\overline{D}} u_i^{r_i}, h\right) \\
&= e\left(A, h^{(\theta+\mu)c}\right) e\left(g_1^{-c} g_2^{-c\cdot y} \prod_{i=0}^{n} u_i^{-c\cdot a_i}, h\right) e\left(D_2^{r_\mu} u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} \prod_{i\in\overline{D}} u_i^{r_i}, h\right) \\
&= e\left(\left(g_1 g_2^{y} \prod_{i=0}^{n} u_i^{a_i}\right)^{1/(\theta+\mu)}, h^{(\theta+\mu)c}\right) e\left(g_1^{-c} g_2^{-c\cdot y} \prod_{i=0}^{n} u_i^{-c\cdot a_i}, h\right) e\left(D_2^{r_\mu} u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} \prod_{i\in\overline{D}} u_i^{r_i}, h\right) \\
&= e\left(D_2^{r_\mu} u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} \prod_{i\in\overline{D}} u_i^{r_i}, h\right)
\end{aligned}
$$

DAS Protocol: Presentation

❖ R_2

$$= e(D_2,h)^{s_\mu} e(u_0,h_\theta)^{s_\alpha} e(u_0,h)^{s_\gamma} e(g_2,h)^{s_y} e\left(u_{\bar{i}},h\right)^{s_{\bar{i}}} \cdot \left(e(D_2,h_\theta)\left(\prod\nolimits_{i\in DI} e(u_i,h)^{-s_i}\right) e(g_1,h)^{-1}\right)^c$$

$$= e(D_2,h^{s_\mu}h_\theta^c) e(u_0,h_\theta)^{r_\alpha - c\cdot\alpha} e(u_0,h)^{r_\gamma - c\cdot\gamma} e\left(g_1^{-c} g_2^{r_y - c\cdot y} \prod\nolimits_{i\in\bar{D}} u_i^{r_i - c\cdot a_i}, h\right) \left(e\left(\prod\nolimits_{i\in DI} u_i^{-c\cdot a_i}, h\right)\right.$$

$$= e(D_2,h^{r_\mu + c\cdot\mu} h_\theta^c) e\left(u_0,h^\theta\right)^{-c\cdot\alpha} e(u_0,h)^{-c\cdot(\alpha\mu+z)} e\left(g_1^{-c} g_2^{-c\cdot y} \prod\nolimits_{i=1}^{n} u_i^{-c\cdot a_i}, h\right) e(u_0,h_\theta)^{r_\alpha} e\left(g_2^{r_y} u_0^{r_\gamma} \prod\nolimits_{i\in\bar{D}} u_i^{r_i}, h\right)$$

$$= e\left(D_2,h^{r_\mu} h^{(\theta+\mu)c}\right) e(u_0,h)^{-c(\alpha\theta+\alpha\mu+z)} e\left(g_1^{-c} g_2^{-c\cdot y} \prod\nolimits_{i=1}^{n} u_i^{-c\cdot a_i}, h\right) e\left(u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} \prod\nolimits_{i\in\bar{D}} u_i^{r_i}, h\right)$$

$$= e\left(A\cdot u_0^\alpha, h^{(\theta+\mu)c}\right) e(u_0,h)^{-c\alpha(\theta+\mu)} e(u_0,h)^{-ca_0} e\left(g_1^{-c} g_2^{-c\cdot y} \prod\nolimits_{i=1}^{n} u_i^{-c\cdot a_i}, h\right) e\left(D_2^{r_\mu} u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} \prod\nolimits_{i\in\bar{D}} u_i^{r_i}, h\right)$$

$$= e\left(A, h^{(\theta+\mu)c}\right) e\left(g_1^{-c} g_2^{-c\cdot y} \prod\nolimits_{i=0}^{n} u_i^{-c\cdot a_i}, h\right) e\left(D_2^{r_\mu} u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} \prod\nolimits_{i\in\bar{D}} u_i^{r_i}, h\right)$$

$$= e\left(\left(g_1 g_2^y \prod_{i=0}^{n} u_i^{a_i}\right)^{\frac{1}{\theta+\mu}}, h^{(\theta+\mu)c}\right) e\left(g_1^{-c} g_2^{-c\cdot y} \prod\nolimits_{i=0}^{n} u_i^{-c\cdot a_i}, h\right) e\left(D_2^{r_\mu} u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} \prod\nolimits_{i\in\bar{D}} u_i^{r_i}, h\right)$$

$$= e\left(D_2^{r_\mu} u_\theta^{r_\alpha} g_2^{r_y} u_0^{r_\gamma} u_{\bar{i}}^{r_{\bar{i}}}, h\right)$$

EZID Protocol: Symbols and Terms

Symbols and Terms	Explanation
Ipk	- Issuer's Public Key - Ipk=$(e, g, g_1, g_2, u, u_\theta = u^\theta, d, u_0, u_1, \ldots, u_n, h, h_\theta = h^\theta, H)$
usk	- User Private Key $a_0 = z$, Attribute List $(a_1, \ldots, a_n)$, Issuer's Signature $\sigma = (A, \mu, y)$ - usk=$(\vec{a} = (a_0 = z, a_1, \ldots, a_n), \sigma = (A, \mu, y))$
VC (Verifiable Credential)	- Issued to the user through the VC Issuance Protocol - User's attribute list $(a_1, \ldots, a_n)$ and Issuer's signature for them - $\sigma = (A, \mu, y)$
$s \xleftarrow{\$} S$	- Select an element s uniformly at random from the set S
DI	- Set of attribute indices selected for the "selective disclosure" feature in the VC Presentation phase - DI=$\mathrm{DI}_D \cup \mathrm{DI}_R$
DI_D	- Set of attribute indices selected for the "selective disclosure" feature in the VC Presentation phase that are directly exposed
DA	- Set of pairs of selected attribute indices and proof-related parameters for the "selective disclosure" feature in the VC Presentation phase
$\overline{D}$	- $\overline{D} = [1, n] \backslash \mathrm{DI}$
D^*	- $D^* = \overline{D} \cup \mathrm{DI}_R = [1, n] \backslash \mathrm{DI}_D$

Thank you