Brief Announcement: Anonymous Credentials Secure to Ephemeral Leakage

Łukasz Krzywiecki, Marta Wszoła, Mirosław Kutyłowski

Department of Computer Science
Faculty of Fundamental Problems of Technology
Wrocław University of Science and Technology

2017 International Symposium on Cyber Security, Cryptography and Machine Learning

CSCML 2017, Be'er Sheva, Israel

Anonymous credentials

Credentials System

a scheme involving three parties:

- User – proves his attributes,
- Issuer – certifies attributes,
- Verifier – accepts or rejects the proof

Attribures of the user

- age,
- sex,
- citizenship,
- role, ...

User do not reveal its identity.

Camenisch-Lysyanskaya Construction (CL)

Set of attributes

- $m_1, m_2, \ldots, m_l$ denoted as $\{m\}_0^l$

Asymmetric cryptography setup

- $\texttt{Issuer}(x,\ y,\ \{z\}_1^l)$ has a long term **secret key**:
- $\texttt{Verifier}(X, Y, \{Z_i\}_1^l)$ has the **public key**

Zero Knowledge Proof, Unlinkability

- the verifier is convinced,
- gets no information about the user's attributes.
- do not link the protocol runs with the particular user.

Issue Protocol

Four rounds

- **commitment**: the `User` sends a commitment to attributes and to ephemeral values.
- **challenge**: the `Issuer` sends random challenge.
- ***response***: the prover sends the result of some computations over the challenge, the secret and the ephemeral value .
- ***sign***: the `Issuer` sends the signature over the attributes, (certificate).

Proof of knowledge

The first three - proof of knowledge of the attributes

Issue protocol

$\texttt{User}(\{m\}_0^l)$		$\texttt{Issuer}(x,\ y,\ \{z\}_1^l)$
$M = g^{m_0} \Pi_{i=1}^{l} Z_i^{m_i}$		
$(r_0, \ldots r_l) \leftarrow_\$ \mathbb{Z}_q$		
$T = g^{r_0}\ \Pi_{i=1}^{l} Z_i^{r_i}$	$\xrightarrow{M,\ T}$	$c \leftarrow_\$ \mathbb{Z}_q$
	$\xleftarrow{c}$	
$\forall_{i \in \{0,\ldots,l\}}\ s_i = r_i - cm_i$	$\xrightarrow{\{s_i\}_0^l}$	$T \stackrel{?}{=} M^c\ g^{s_0}\ \Pi_{i=1}^{l} Z_i^{s_i}$
		$a_0 \leftarrow_\$ \mathbb{Z}_q,\ A_0 = g^{a_0}$
		$\forall_{i \in \{1,\ldots,l\}}\ A_i = A_0^{z_i}$
		$\forall_{i \in \{0,\ldots,l\}}\ B_i = A_i^{y}$
$\mathrm{Store}(\{A_i\}_0^l,\ \{B_i\}_0^l,\ C)$	$\xleftarrow{\{A_i\}_0^l,\ \{B_i\}_0^l,\ C}$	$C = A_0^x\ M^{a_0 xy}$

Figure: CL system: issuing a credential.

Attribute Verification Protocol

Three rounds

- **commitment**: the `User` sends a commitment to credentials and to ephemeral values.
- **challenge**: the `Verifier` sends random challenge.
- ***response***: the prover sends the result of some computations over the challenge, the credentials and the ephemeral value .

Attribute Verification Protocol

$\mathtt{User}(\{m_i\}_0^l, \{A_i\}_0^l, \{B_i\}_0^l,\ C)$		$\mathtt{Verifier}(X, Y, \{Z_i\}_1^l)$
$(r', r'', r_a, r_0, \dots, r_l) \leftarrow_{\$} \mathbb{Z}_q$		
$\forall_{i\in\{0,\dots,l\}}\ \tilde{A}_i = A_i^{r'}, \tilde{B}_i = B_i^{r'}$		
$\tilde{C} = C^{r'r''}$		
$\hat{t} = \hat{e}(X, \tilde{A}_0)^{r_a}\, \Pi_{i=0}^{l} \hat{e}(X, \tilde{B}_i)^{r_i}$	$\xrightarrow{\{\tilde{A}_i\}_0^l, \{\tilde{B}_i\}_0^l, \tilde{C}, \hat{t}}$	$\forall_{i\in\{1,\dots,l\}} \hat{e}(\tilde{A}_0, Z_i) \stackrel{?}{=} \hat{e}(g, \tilde{A}_i)$
		$\forall_{i\in\{0,\dots,l\}}\ \hat{e}(\tilde{A}_i, Y) \stackrel{?}{=} \hat{e}(g, \tilde{B}_i)$
$s_a = r_a - cr''$	$\xleftarrow{c}$	$c \leftarrow_{\$} \mathbb{Z}_q$
$\forall_{i\in\{0,\dots,l\}}\ s_i = r_i - cm_i r''$	$\xrightarrow{s_a, \{s_i\}_0^l}$	$\hat{t} \stackrel{?}{=} \hat{e}(g, \tilde{C})^c \hat{e}(X, \tilde{A}_0)^{s_a} \Pi_{i=0}^{l} \hat{e}(X, \tilde{B}_i)^{s_i}$

Figure: CL system: attribute verification.

Device based authentication

Device

Small hardware which *securely* store the authentication keys inside (e.g smartcards).

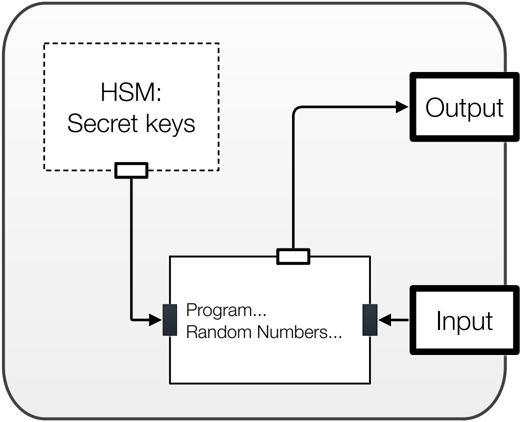
Adversaries Attacks

- tries to extract what was put inside,
- tries to manipulate what is inside,
- ...

Common threats:

- invasive attack,
- power analysis,
- emission of radiation,
- ...

Typical Device Architecture
Device Monolitic Architecture



Regular CL

Ephemeral Setup Attack

Attack on Issue Protocol

- set r_i,
- capture $s_i = r_i - cm_i$
- extract m_i

Attack on Verification Protocol

- set r_i, r'',
- capture $s_i = r_i - cm_i r''$
- extract m_i

Chosen Prover Ephemeral

Model

Security experiment

The experiment $\mathtt{Exp}_{\mathsf{IS}}^{\mathsf{CPE},\lambda,\ell}$:

Init stage System setup.

Query stage $\mathcal{A}$ runs a polynomial number ℓ of $\pi(\mathtt{User}^{\bar{x}}, ...)$ collecting view v, where $\bar{x}_i \in \{\bar{x}_1, \ldots, \bar{x}_\ell\}$ are injected

Impersonation stage $\mathcal{A}$ runs the protocol $\pi(\mathcal{A}(\mathsf{pk}, v), ...)$

Adversary advantage

The advantage of $\mathcal{A}$ in the experiment $\mathtt{Exp}_{\mathsf{IS}}^{\mathsf{CPE},\lambda,\ell}$ as **probability of acceptance** in the *impersonation stage*:

$$\mathbf{Adv}(\mathcal{A}, \mathtt{Exp}_{\mathsf{IS}}^{\mathsf{CPE},\lambda,\ell}) = \Pr[\pi(\mathcal{A}(\mathsf{pk}, v), \ldots) \to 1].$$

The identification scheme is secure if it is negligible in λ.

Security of identification scheme

$\mathcal{A}$ **probability of acceptance** is negligible in λ.

Solution
Shifting computation into exponent

Issue Protocol

instead

$$s_i = r_i - cm_i$$

we compute

$$S_i = \tilde{g}^{r_i - cm_i}$$

for

$$\tilde{g} = g^{\omega}$$

Verification Protocol

instead

$$s_i = r_i - cm_i r''$$

we compute

$$S_i = \overline{X}^{\,r_i - cm_i r''}$$

for

$$\overline{X} = X^{\omega}$$

Modified CL scheme

$\mathtt{User}(\{m_i\}_0^l)$		$\mathtt{Issuer}(x, y, \{z_i\}_1^l)$
$M = g^{m_0} \Pi_{i=1}^l Z_i^{m_i}$ $(r_0, \ldots, r_l) \leftarrow_\$ \mathbb{Z}_q$ $T = g^{r_0} \Pi_{i=1}^l Z_i^{r_i}$	$\xrightarrow{M,\ T}$	$(c, \omega) \leftarrow_\$ \mathbb{Z}_q,\ \tilde{g} = g^\omega$
	$\xleftarrow{c, \tilde{g}}$	
$\forall_{i \in \{0,\ldots,l\}}\ S_i = \tilde{g}^{r_i - c m_i}$	$\xrightarrow{\{S_i\}_0^l}$	$\widehat{e}(\tilde{g}, T/M^c) \stackrel{?}{=} \widehat{e}(S_0, g)\ \prod_{i=1}^l \widehat{e}(S_i, Z_i)$ $a_0 \leftarrow_\$ \mathbb{Z}_q,\ A_0 = g^{a_0}$ $\forall_{i \in \{1,\ldots,l\}}\ A_i = A_0^{z_i}$ $\forall_{i \in \{0,\ldots,l\}}\ B_i = A_i^y$
$\mathrm{Store}(\{A_i\}_0^l,\ \{B_i\}_0^l,\ C)$	$\xleftarrow{\{A_i\}_0^l,\ \{B_i\}_0^l,\ C}$	$C = A_0^x\ M^{a_0 xy}$

Figure: Credential issuance protocol for the modified system.

Krzywiecki, Wszoła, Kutyłowski

Attribute Verification Protocol

User$(\{m_i\}_0^l, \{A_i\}_0^l, \{B_i\}_0^l, C)$ — **Verifier**$(X, Y, \{Z_i\}_1^l)$

$$(r', r'', r_a, r_0, \ldots, r_l) \leftarrow_\$ \mathbb{Z}_q$$
$$\forall_{i \in \{0,\ldots,l\}}\ \tilde{A}_i = A_i^{r'}$$
$$\forall_{i \in \{0,\ldots,l\}}\ \tilde{B}_i = B_i^{r'}$$
$$\tilde{C} = C^{r'r''}$$
$$\hat{t} = \widehat{e}(X, \tilde{A}_0)^{r_a} \Pi_{i=0}^{l} \widehat{e}(X, \tilde{B}_i)^{r_i}$$

User → Verifier: $\{\tilde{A}_i\}_0^l, \{\tilde{B}_i\}_0^l, \tilde{C}, \hat{t}$

Verifier:

$$\forall_{i \in \{1,\ldots,l\}}\ \widehat{e}(\tilde{A}_0, Z_i) \stackrel{?}{=} \widehat{e}(g, \tilde{A}_i)$$
$$\forall_{i \in \{0,\ldots,l\}}\ \widehat{e}(\tilde{A}_i, Y) \stackrel{?}{=} \widehat{e}(g, \tilde{B}_i)$$
$$(\omega, c) \leftarrow_\$ \mathbb{Z}_q$$
$$\overline{X} = X^{\omega}$$

Verifier → User: $c, \overline{X}$

$$s_a = r_a - cr''$$
$$\forall_{i \in \{0,\ldots,l\}}\ S_i = \overline{X}^{\,r_i - cm_i r''}$$

User → Verifier: $s_a, \{S_i\}_0^l$

Verifier:

$$\hat{t}^{\omega} \stackrel{?}{=} \widehat{e}(g^{\omega c}, \tilde{C})\widehat{e}(\overline{X}, \tilde{A}_0)^{s_a} \Pi_{i=0}^{l} \widehat{e}(S_i, \tilde{B}_i)$$

Figure: CL system: attribute verification.

Security Assumption

Assumption (modLRSW Assumption)

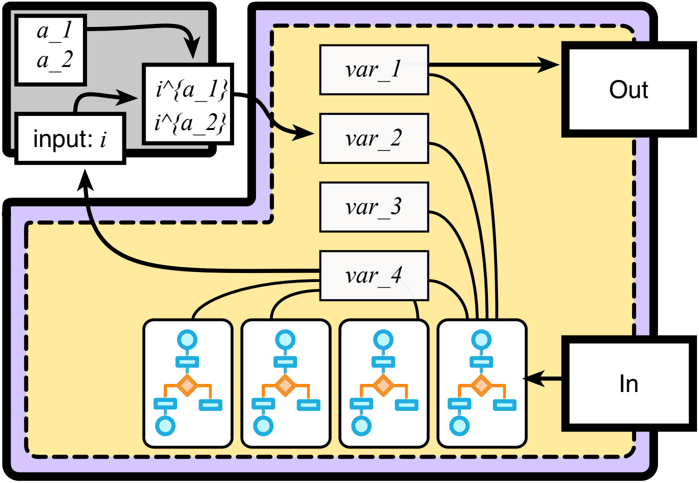
Let $\mathbb{G}$ *be a cyclic group with generator* g *and prime order* q*. Let* $A = g^a, B = g^b \in \mathbb{G}$*. Let* $\mathrm{Par} = (\mathbb{G}, g, q, A, B)$ *denote public parameters. Let* $\mathcal{O}_{AB}(\cdot)$ *be an oracle that on input* $m \in \mathbb{Z}_q$ *outputs* $(r,\ r^b,\ r^{a+mab})$*, where* r *is a random* $\mathbb{G}$ *element.*

$$\Pr\left[\begin{array}{c}(h^{m'}, (x,\ y,\ z)) \leftarrow \mathcal{A}^{\mathcal{O}_{AB}(\cdot)}(\mathrm{Par}, h) \\ \text{s.t. } m' \notin Q \wedge x \in \mathbb{G} \wedge y = x^b \wedge z = x^{a+m'ab}\end{array}\right] < \epsilon,$$

where $Q = \{m_i\}$ *denotes the set of messages* m_i *queried to* $\mathcal{O}_{A,B}(\cdot)$ *oracle.*

Device model

HSM with minimal functionality



Computations with unreliable devices

Possible Advantages

”Gray” Secure Module

1. user retain ”Gray” Secure Module
2. ”Gray” Secure Module – black box

”Yellow” Insecure Module

1. yellow part can be outsourced to unreliable devices
2. yellow part – white box

Adversary cannot:

- extract long term secret keys,
- impersonate user

Thanks

Thank You