Brief Announcement Anonymous Deniable Identification in Ephemeral Setup & Leakage Scenarios

Łukasz Krzywiecki, Mirosław Kutyłowski, Marcin Słowik, Jakub Pezda

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

CSCML 2019, Beer-Sheva, Israel

General Construction

Identification Scheme (AS)

a scheme involving two parties:

- prover – proves his identity,
- verifier – accepts or rejects the proof

Asymmetric cryptography setup

- the prover has a k-of-n **secret keys**: $\{\mathrm{sk}_j\}_1^k$
- the verifier has all n the **public keys**: $\{\mathrm{pk}_i\}_1^n$

Zero Knowledge Proof

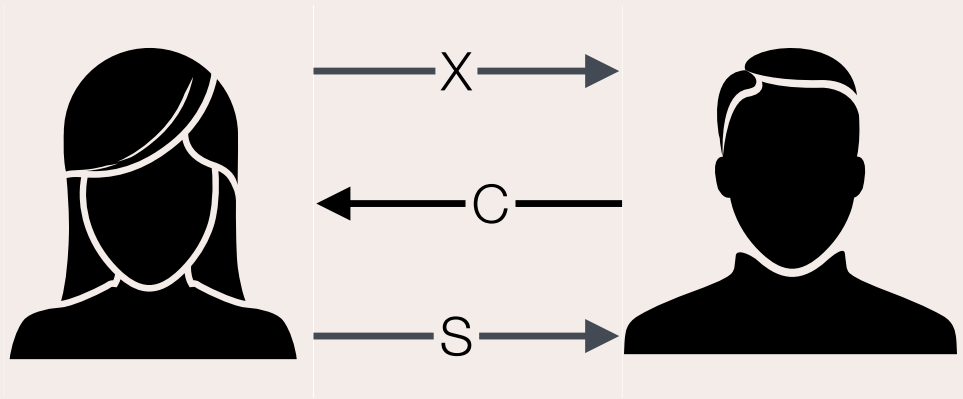
- the verifier is convinced,
- gets no information about the prover's secret.

General Construction

$k - of - n$ Anonimity

$\{sk_j\}_1^k, \{pk_i\}_1^n$ $\{pk_i\}_1^n$

Prover Verifier



- x for commitment
- c for challenge
- s for proof

Deniability

Deniable Identification

Simulatability: Assuming the protocol with the honest verifier. Anyone with the public key can produce the transcript itself.

Distinguisher

Cannot tell

- whether the transcript was a result of the regular protocol execution.
- or the transcript was simulated.

even if it was given the secret key.

Device based authentication

Device (Prover, Verifier)

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

Attacks

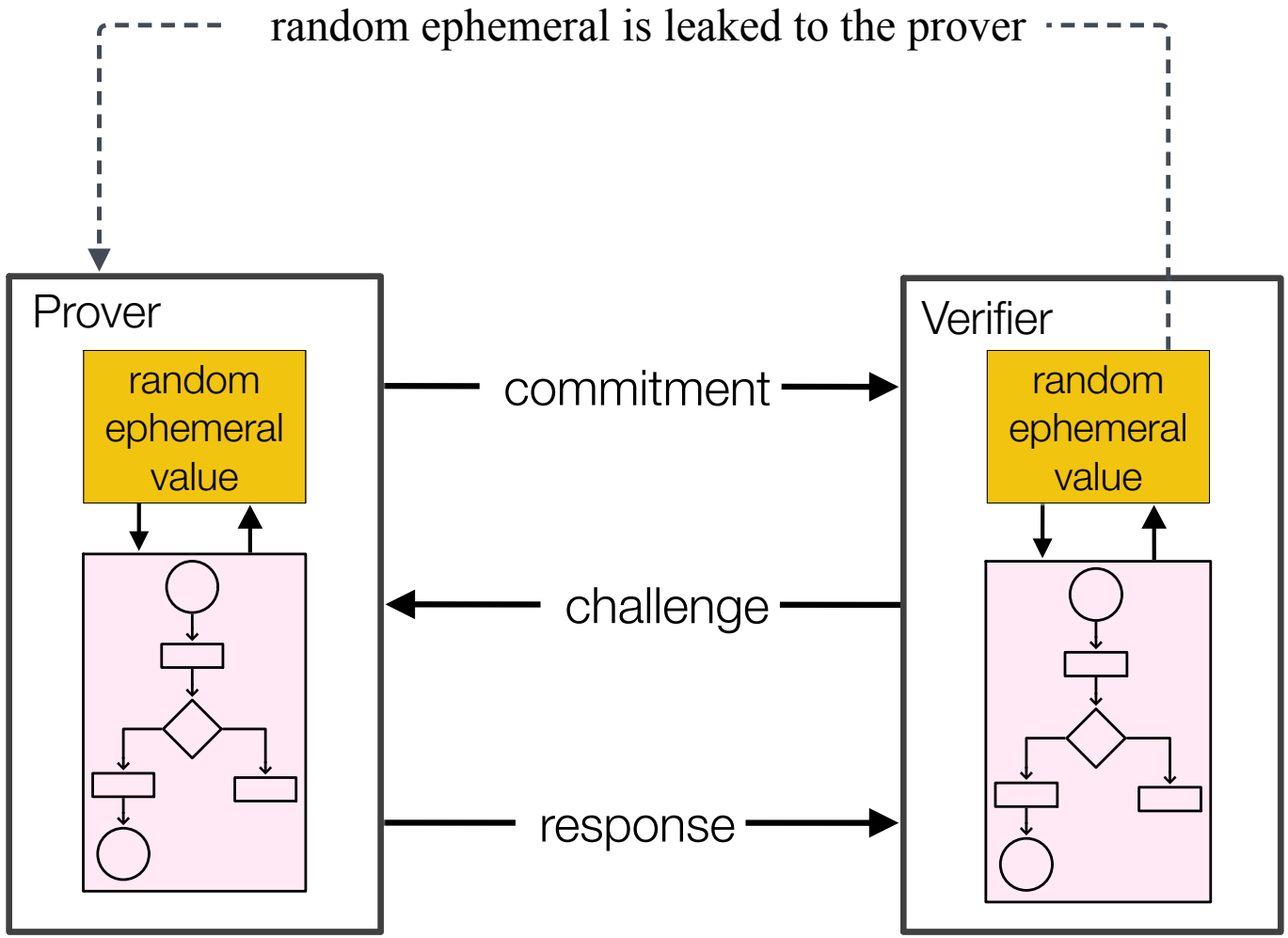
Adversaries tries to extract what was put inside.

Common threats:

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

Device based authentication

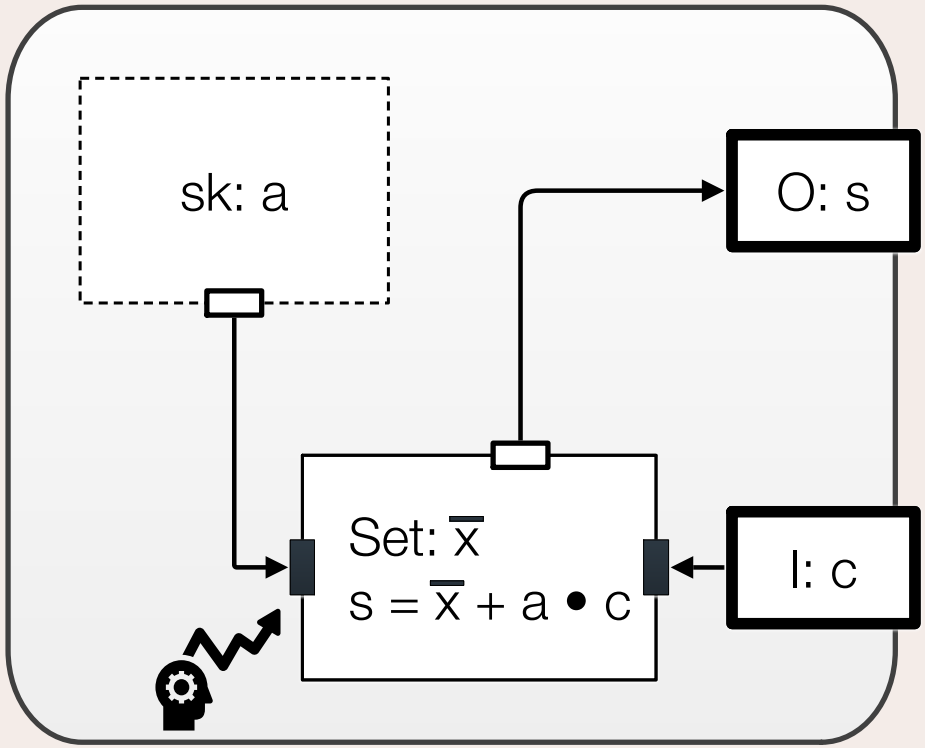
Prover and Verifier devices



Schnorr based identification scheme

Chosen Prover Ephemeral

Attack - subliminal setting of ephemerals



Schnorr IS is not secure if $\bar{x}$ is known to the adversary.
$\mathcal{A}$ can easily compute the secret key $a = (s - \bar{x})/c$.

Our construction

- deniable
- k-of-n anonymous
- secure against epehemeral setup in prover devices
- secure against epehemeral leakage in verifier devices

Commitment

1. $\mathcal{P}$: $X_Z = \{X_i\}_Z$, s.t. $s_i, c_i \leftarrow_\$ \mathbb{Z}_q^*$, $X_i = g_1^{s_i}/A_i^{c_i}$ for each $i \in Z$
2. $\mathcal{P}$: $X_J = \{X_j\}_J$, s.t. for each $j \in J$ compute $x_j \leftarrow_\$ \mathbb{Z}_q^*$, $X_j = g_1^{x_j}$
3. $\mathcal{P}$: sends $X = X_Z \cup X_J$ to the verifier $\mathcal{V}$.

Challenge

1. $\mathcal{V}$: sets $P_C = \{(x_i, y_i)\}_1^k$, where each pair $x_i, y_i \leftarrow_\$ \mathbb{Z}_q^*$.

Our construction

Response

1. $\mathcal{P}$: set $P_Z = \{(x_i, y_i)\}_Z$, s.t. $x_i = \mathcal{H}(X_i)$, $y_i = c_i$ for $i \in Z$.
2. $\mathcal{P}$: sets $P = P_C \cup P_Z$, interpolates a polynomial $L_P(x)$ for P.
3. $\mathcal{P}$: computes $\hat{g}_2 = \mathcal{H}_{g_2}(X, P_C)$
4. $\mathcal{P}$: for each $j \in J$, computes $c_j = L_P(\mathcal{H}(X_j))$, $s_j = x_j + a_j c_j$.
5. $\mathcal{P}$: for $i \in I$ sets $S_i = \hat{g}_2^{s_i}$, sends $\{c_i, S_i\}_1^n$ to the verifier $\mathcal{V}$.

Verification

1. $\mathcal{V}$: sets $\bar{P} = \{(x_i, y_i)\}_1^n$, s.t. $x_i = \mathcal{H}(X_i)$, $y_i = c_i$ for each $i \in I$.
2. $\mathcal{V}$: interpolates a polynomial $L_{\bar{P}}(x)$ for points $\bar{P}$.
3. $\mathcal{V}$: accepts the verification iff $(\forall_{\{i \in I\}}\ \hat{e}(g_1, S_i) = \hat{e}\left(X_i A_i^{c_i}, \hat{g}_2\right)$ and $(\forall_{\{(x_i, y_i) \in P_C\}}\ L_{\bar{P}}(x_i) = y_i)$.

Thanks

Thank You