Machine-Checking Unforgeability Proofs for Signature Schemes with Tight Reductions to the Computational Diffie-Hellman Problem

Authors: Dr Francois Dupressoir (University of Bristol, f.dupressoir@bristol.ac.uk) and Sara Zain (University of Bristol, lu20465@bristol.ac.uk)
Presenter: Sara Zain

34th IEEE Computer Security Foundations Symposium
June 21-24, 2021 - Virtual Conference

EDL(EUROCRYPT 2003) and Chevallier-Mames(CM)(CRYPTO 2005) signature schemes

- The first machine-checked proofs for signature schemes based on Discrete Logarithm (DL) problem.

The EDL Scheme

$\mathsf{EDL}^{\mathcal{H},\mathcal{G}}_{\mathbb{G},g,q}$

$\mathsf{KGen}()$

$\mathsf{sk} \leftarrow_{\$} \mathbb{F}_q$

$\textbf{return } (\mathsf{sk}, g^{\mathsf{sk}})$

$\mathsf{Ver}_{\mathsf{pk}}(\mathsf{m}, (\mathsf{z}, \mathsf{r}, \mathsf{s}, \mathsf{c}))$

$\boxed{\mathsf{h} \leftarrow \mathcal{H}(\mathsf{m}, \mathsf{r})}$

$\mathsf{u} \leftarrow g^{\mathsf{s}}\mathsf{pk}^{-\mathsf{c}}$

$\mathsf{v} \leftarrow \mathsf{h}^{\mathsf{s}}\mathsf{z}^{-\mathsf{c}}$

$\mathsf{c}' \leftarrow \mathcal{G}(g, \mathsf{h}, \mathsf{pk}, \mathsf{z}, \mathsf{u}, \mathsf{v})$

$\textbf{return } \mathsf{c} = \mathsf{c}'$

$\mathsf{Sign}_{\mathsf{sk}}(\mathsf{m})$

$\boxed{\mathsf{r} \leftarrow_{\$} d_{\mathcal{N}}}$

$\mathsf{h} \leftarrow \mathcal{H}(\mathsf{m}, \mathsf{r})$

$\boxed{\mathsf{z} \leftarrow \mathsf{h}^{\mathsf{sk}}}$

$\mathsf{k} \leftarrow_{\$} \mathbb{F}_q$

$\mathsf{u} \leftarrow g^{\mathsf{k}}$

$\mathsf{v} \leftarrow \mathsf{h}^{\mathsf{k}}$

$\mathsf{c} \leftarrow \mathcal{G}(g, \mathsf{h}, g^{\mathsf{sk}}, \mathsf{z}, \mathsf{u}, \mathsf{v})$

$\mathsf{s} \leftarrow \mathsf{k} + \mathsf{c} \cdot \mathsf{sk}$

$\textbf{return } (\mathsf{z}, \mathsf{r}, \mathsf{s}, \mathsf{c})$

NIZK proof of DL equality

$$\mathcal{H} \in \mathcal{M} \times \mathcal{N} \rightarrow \boldsymbol{G},$$
$$\mathcal{G} \in \boldsymbol{G}^6 \rightarrow \boldsymbol{F}_q$$

$\mathcal{M}$: set of msgs,
$\mathcal{N}$: set of nonces,
$\boldsymbol{G}$: cyclic group,
$\boldsymbol{F}_q$: prime field

Definitions and the advantages

$$\underline{\mathsf{Exp}^{\mathsf{euf\text{-}cma}}_{\mathcal{H},\mathcal{G},\mathcal{S},\mathcal{F}}()}$$
$$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathcal{S}.\mathsf{KGen}()$$
$$(\tilde{\mathsf{m}},\tilde{\sigma}) \leftarrow \mathcal{F}^{\mathcal{H},\mathcal{G},\mathcal{S}.\mathsf{Sign}_{\mathsf{sk}}(\cdot)}(\mathsf{pk})$$
$$\mathsf{b} \leftarrow \mathcal{S}.\mathsf{Ver}_{\mathsf{pk}}(\tilde{\mathsf{m}},\tilde{\sigma})$$

$$\underline{\mathsf{Exp}^{\mathsf{cdh}}_{\mathcal{A}}(G, g_G, n)}$$
$$\mathsf{a} \leftarrow_{\$} \mathbb{F}_q$$
$$\mathsf{b} \leftarrow_{\$} \mathbb{F}_q$$
$$\mathsf{r} \leftarrow \mathcal{A}_{G,g_G,n}(g_G^{\mathsf{a}}, g_G^{\mathsf{b}})$$

$$\mathsf{Adv}^{\mathsf{euf\text{-}cma}}_{\mathcal{H},\mathcal{G},\mathcal{S}}(\mathcal{A}) := \Pr\left[\mathsf{Exp}^{\mathsf{euf\text{-}cma}}_{\mathcal{H},\mathcal{G},\mathcal{S},\mathcal{A}}() : \mathsf{b} \wedge \tilde{\mathsf{m}} \notin \mathcal{Q}_{\mathcal{S}}\right]$$

$$\mathsf{Adv}^{\mathsf{cdh}}_{G,g_G,n}(\mathcal{A}) := \Pr\left[\mathsf{Exp}^{\mathsf{cdh}}_{\mathcal{A}}(G, g_G, n) : \mathsf{r} = g_G^{\mathsf{ab}}\right]$$

$$Adv^{euf-cma}_{EDL}(A) \leq Adv^{cdh} + \varepsilon$$

Intuition

$\mathcal{A}^{\mathcal{F}}_{\mathbb{G},g,q}(\mathsf{pk}, \mathsf{g_b})$

var $\mathsf{H} \in \mathcal{M} \times \mathcal{N} \rightharpoonup \mathbb{G} \times \mathbb{F}_q$
var $\mathsf{G} \in \mathbb{G}^6 \rightharpoonup \mathbb{F}_q$

Embed CDH

Simulates NIZK proof

Oracle simulation

$\mathcal{H}(\mathsf{x})$
$\mathsf{d} \leftarrow\!\!\$\ \mathbb{F}_q$
if $(\mathsf{x}) \notin \mathsf{H}$
$\lfloor\ \mathsf{H}[\mathsf{x}] \leftarrow (\mathsf{g_b} g^{\mathsf{d}}, \mathsf{d})$
return $\pi_1(\mathsf{H}[\mathsf{x}])$

$\mathcal{G}(\mathsf{x})$
$\mathsf{c} \leftarrow\!\!\$\ \mathbb{F}_q$
if $\mathsf{x} \notin \mathsf{G}$
$\lfloor\ \mathsf{G}[\mathsf{x}] \leftarrow c$
return $\mathsf{G}[\mathsf{x}]$

$\mathsf{Sign}(\mathsf{m})$
$\mathsf{r} \leftarrow\!\!\$\ d_{\mathcal{N}}$
$\mathsf{d} \leftarrow\!\!\$\ \mathbb{F}_q$
$\mathsf{H}[\mathsf{m}, \mathsf{r}] \leftarrow (g^{\mathsf{d}}, \mathsf{d})$
$\mathsf{c} \leftarrow\!\!\$\ \mathbb{F}_q$
$\mathsf{s} \leftarrow\!\!\$\ \mathbb{F}_q$
$\mathsf{u} \leftarrow g^{\mathsf{s}} \mathsf{pk}^{-\mathsf{c}}$
$\mathsf{v} \leftarrow \mathsf{g}^{\mathsf{ds}} \mathsf{pk}^{-\mathsf{dc}}$
$\mathsf{G}[g, \mathsf{g}^{\mathsf{d}}, \mathsf{pk}, \mathsf{pk}^{\mathsf{d}}, \mathsf{u}, \mathsf{v}] \leftarrow c$
return $(\mathsf{z}, \mathsf{r}, \mathsf{s}, \mathsf{c})$

$(\tilde{\mathsf{m}}, (\tilde{\mathsf{z}}, \tilde{\mathsf{r}}, \_, \_)) \leftarrow \mathcal{F}^{\mathcal{H},\mathcal{G},\mathsf{Sign}}(\mathsf{pk})$
$\_ \leftarrow \mathcal{H}(\tilde{\mathsf{m}}, \tilde{\mathsf{r}})$ / This is to ensure $(\tilde{\mathsf{m}}, \tilde{\mathsf{r}}) \in \mathsf{H}$
$\mathsf{d} \leftarrow \pi_2(\mathsf{H}[\tilde{\mathsf{m}}, \tilde{\mathsf{r}}])$
return $\tilde{\mathsf{z}} \cdot \mathsf{pk}^{-\mathsf{d}}$

Formal proof in 4 steps

1) Refactoring
2) Embedding
3) Simulation
4) Reduction

Formalisation

- Machine-checked proofs
  - Emerging approach, ensures the correctness of reasoning steps (smt solvers & automated theorem provers).
- EasyCrypt
  - Follows the code-based, game-based approach to reductionist argument
  - Security goals & assumptions are modelled as probabilistic programs (called experiments/games)

Overview of the sequence of games & the Shim

$$\mathsf{Game}^{\mathsf{EDL}}_{\mathcal{H},\mathcal{G},\mathcal{S},\mathcal{F}}()$$

$$\begin{array}{l}
\mathsf{sk} \leftarrow_{\$} \mathbb{F}_q \\
\mathsf{b} \leftarrow_{\$} \mathbb{F}_q \\
\mathsf{pk} \leftarrow g^{\mathsf{sk}} \\
\mathsf{g_b} \leftarrow g^{\mathsf{b}} \\
(\tilde{\mathsf{m}}, (\tilde{\mathsf{z}}, \tilde{\mathsf{r}}, \tilde{\mathsf{s}}, \tilde{\mathsf{c}})) \leftarrow \mathcal{F}^{\mathcal{H},\mathcal{G},\mathcal{S}}(\mathsf{pk}) \\
\mathsf{h} \leftarrow \mathcal{H}(\tilde{\mathsf{m}}, \tilde{\mathsf{r}}) \\
\mathsf{u} \leftarrow g^{\tilde{\mathsf{s}}}\mathsf{pk}^{-\tilde{\mathsf{c}}} \\
\mathsf{v} \leftarrow \mathsf{h}^{\tilde{\mathsf{s}}}\mathsf{pk}^{-\tilde{\mathsf{c}}} \\
\mathsf{c} \leftarrow \mathcal{G}(g, \mathsf{h}, \mathsf{pk}, \tilde{\mathsf{z}}, \mathsf{u}, \mathsf{v}) \\
\mathsf{win} \leftarrow \tilde{\mathsf{c}} = \mathsf{c} \wedge \tilde{\mathsf{m}} \notin \mathcal{Q}_{\mathcal{S}}
\end{array}$$

The EDL proof Shim

$$\mathcal{S}_0(\mathsf{m})$$

$$\begin{array}{l}
\mathsf{r} \leftarrow_{\$} \mathcal{N} \\
\mathsf{h} \leftarrow \mathcal{H}(\mathsf{m}, \mathsf{r}) \\
\mathsf{z} \leftarrow \mathsf{h}^{\mathsf{sk}} \\
\mathsf{k} \leftarrow_{\$} \mathbb{F}_q; \mathsf{u} \leftarrow g^{\mathsf{k}}; \mathsf{v} \leftarrow \mathsf{h}^{\mathsf{k}} \\
\mathsf{c} \leftarrow \mathcal{G}(g, \mathsf{h}, g^{\mathsf{sk}}, \mathsf{z}, \mathsf{u}, \mathsf{v}) \\
\mathsf{s} \leftarrow \mathsf{k} + \mathsf{c} \cdot \mathsf{sk} \\
\mathbf{return}\ (\mathsf{z}, \mathsf{r}, \mathsf{s}, \mathsf{c})
\end{array}$$

$$\mathcal{H}(\mathsf{x})$$

$$\begin{array}{l}
\mathsf{h} \leftarrow_{\$} \mathbb{G} \\
\mathbf{if}\ \mathsf{x} \notin \mathsf{H} \\
\quad \lfloor\ \mathsf{H}[\mathsf{x}] \leftarrow \mathsf{h} \\
\mathbf{return}\ \mathsf{H}[\mathsf{x}]
\end{array}$$

$$\mathcal{G}(\mathsf{x})$$

$$\begin{array}{l}
\mathsf{c} \leftarrow_{\$} \mathbb{F}_q \\
\mathbf{if}\ \mathsf{x} \notin \mathsf{G} \\
\quad \lfloor\ \mathsf{G}[\mathsf{x}] \leftarrow \mathsf{c} \\
\mathbf{return}\ \mathsf{G}[\mathsf{x}]
\end{array}$$

$$\mathcal{S}_1(\mathsf{m})$$

$$\begin{array}{l}
\mathsf{r} \leftarrow_{\$} \mathcal{N}; \mathsf{bad}_{\mathcal{H}} \leftarrow \mathsf{bad}_{\mathcal{H}} \vee (\mathsf{m}, \mathsf{r}) \in \mathsf{H} \\
\boxed{\begin{array}{l} \mathsf{d} \leftarrow_{\$} \mathbb{F}_q; \mathsf{h} \leftarrow g^{\mathsf{d}} \\ \mathsf{H}[\mathsf{m}, \mathsf{r}] \leftarrow (\mathsf{h}, \mathsf{d}) \end{array}} \\
\mathsf{z} \leftarrow \mathsf{h}^{\mathsf{sk}} \\
\mathsf{k} \leftarrow_{\$} \mathbb{F}_q; \mathsf{u} \leftarrow g^{\mathsf{k}}; \mathsf{v} \leftarrow \mathsf{h}^{\mathsf{k}} \\
\mathsf{bad}_{\mathcal{G}} \leftarrow \mathsf{bad}_{\mathcal{G}} \vee \\
\qquad (g, \mathsf{h}, g^{\mathsf{sk}}, \mathsf{z}, \mathsf{u}, \mathsf{v}) \in \mathsf{G} \\
\mathsf{c} \leftarrow \mathcal{G}(g, \mathsf{h}, g^{\mathsf{sk}}, \mathsf{z}, \mathsf{u}, \mathsf{v}) \\
\mathsf{s} \leftarrow \mathsf{k} + \mathsf{c} \cdot \mathsf{sk} \\
\mathbf{return}\ (\mathsf{z}, \mathsf{r}, \mathsf{s}, \mathsf{c})
\end{array}$$

$$\mathcal{H}'(\mathsf{x})$$

$$\begin{array}{l}
\mathsf{d} \leftarrow_{\$} \mathbb{F}_q \\
\mathbf{if}\ \mathsf{x} \notin \mathsf{H} \\
\quad \lfloor\ \mathsf{H}[\mathsf{x}] \leftarrow (\mathsf{g_b} g^{\mathsf{d}}, \mathsf{d}) \\
\mathbf{return}\ \pi_1(\mathsf{H}[\mathsf{x}])
\end{array}$$

$$\mathcal{S}_2(\mathsf{m})$$

$$\begin{array}{l}
\mathsf{r} \leftarrow_{\$} \mathcal{N} \\
\mathsf{d} \leftarrow_{\$} \mathbb{F}_q; \mathsf{h} \leftarrow g^{\mathsf{d}} \\
\mathsf{H}[\mathsf{m}, \mathsf{r}] \leftarrow (\mathsf{h}, \mathsf{d}) \\
\mathsf{z} \leftarrow \mathsf{pk}^{\mathsf{d}} \\
\boxed{\begin{array}{l} \mathsf{c} \leftarrow_{\$} \mathbb{F}_q; \mathsf{s} \leftarrow_{\$} \mathbb{F}_q \\ \mathsf{u} \leftarrow g^{\mathsf{s}}\mathsf{pk}^{-\mathsf{c}}; \mathsf{v} \leftarrow \mathsf{h}^{\mathsf{s}}\mathsf{z}^{-\mathsf{c}} \\ \mathsf{bad}_{\mathcal{G}} \leftarrow \mathsf{bad}_{\mathcal{G}} \vee \\ \qquad (g, \mathsf{h}, \mathsf{pk}, \mathsf{z}, \mathsf{u}, \mathsf{v}) \in \mathsf{G} \\ \mathsf{G}[g, \mathsf{h}, \mathsf{pk}, \mathsf{z}, \mathsf{u}, \mathsf{v}] \leftarrow \mathsf{c} \end{array}} \\
\mathbf{return}\ (\mathsf{z}, \mathsf{r}, \mathsf{s}, \mathsf{c})
\end{array}$$

Sequence of games

3) Simulation (pRHL judgment)

$\mathcal{S}_1(\mathsf{m})$

$\mathsf{r} \leftarrow\!\!\$\; \mathcal{N};\ \mathsf{bad}_{\mathcal{H}} \leftarrow \mathsf{bad}_{\mathcal{H}} \vee (\mathsf{m},\mathsf{r}) \in \mathsf{H}$
$\mathsf{d} \leftarrow\!\!\$\; \mathbb{F}_q;\ \mathsf{h} \leftarrow g^{\mathsf{d}}$
$\mathsf{H}[\mathsf{m},\mathsf{r}] \leftarrow (\mathsf{h},\mathsf{d})$
$\mathsf{z} \leftarrow \mathsf{h}^{\mathsf{sk}}$
$\mathsf{k} \leftarrow\!\!\$\; \mathbb{F}_q;\ \mathsf{u} \leftarrow g^{\mathsf{k}};\ \mathsf{v} \leftarrow \mathsf{h}^{\mathsf{k}}$
$\mathsf{bad}_{\mathcal{G}} \leftarrow \mathsf{bad}_{\mathcal{G}} \vee (g,\mathsf{h},g^{\mathsf{sk}},\mathsf{z},\mathsf{u},\mathsf{v}) \in \mathsf{G}$
$\mathsf{c} \leftarrow \mathcal{G}(g,\mathsf{h},g^{\mathsf{sk}},\mathsf{z},\mathsf{u},\mathsf{v})$
$\mathsf{s} \leftarrow \mathsf{k} + \mathsf{c}\cdot\mathsf{sk}$
return $(\mathsf{z},\mathsf{r},\mathsf{s},\mathsf{c})$

secret key used

$\mathcal{H}'(\mathsf{x})$

$\mathsf{d} \leftarrow\!\!\$\; \mathbb{F}_q$
if $\mathsf{x} \notin \mathsf{H}$
$\quad \mathsf{H}[\mathsf{x}] \leftarrow (\mathsf{g_b} g^{\mathsf{d}}, \mathsf{d})$
return $\pi_1(\mathsf{H}[\mathsf{x}])$

$\mathcal{S}_2(\mathsf{m})$

$\mathsf{r} \leftarrow\!\!\$\; \mathcal{N}$
$\mathsf{d} \leftarrow\!\!\$\; \mathbb{F}_q;\ \mathsf{h} \leftarrow g^{\mathsf{d}}$
$\mathsf{H}[\mathsf{m},\mathsf{r}] \leftarrow (\mathsf{h},\mathsf{d})$
$\mathsf{z} \leftarrow \mathsf{pk}^{\mathsf{d}}$
$\mathsf{c} \leftarrow\!\!\$\; \mathbb{F}_q;\ \mathsf{s} \leftarrow\!\!\$\; \mathbb{F}_q$
$\mathsf{u} \leftarrow g^{\mathsf{s}}\mathsf{pk}^{-\mathsf{c}};\ \mathsf{v} \leftarrow \mathsf{h}^{\mathsf{s}}\mathsf{z}^{-\mathsf{c}}$
$\mathsf{bad}_{\mathcal{G}} \leftarrow \mathsf{bad}_{\mathcal{G}} \vee (g,\mathsf{h},\mathsf{pk},\mathsf{z},\mathsf{u},\mathsf{v}) \in \mathsf{G}$
$\mathsf{G}[g,\mathsf{h},\mathsf{pk},\mathsf{z},\mathsf{u},\mathsf{v}] \leftarrow \mathsf{c}$
return $(\mathsf{z},\mathsf{r},\mathsf{s},\mathsf{c})$

secret key isn't used

Failure event **Bad$\mathcal{G}$**

Oracle$\mathcal{H}$ is the same as S1

$$\Pr\left[\mathsf{Game}^{\mathsf{EDL}}_{\mathcal{H}',\mathcal{G},\mathcal{S}_1,\mathcal{F}}() : \mathsf{bad}_{\mathcal{G}}\right] = \Pr\left[\mathsf{Game}^{\mathsf{EDL}}_{\mathcal{H}',\mathcal{G},\mathcal{S}_2,\mathcal{F}}() : \mathsf{bad}_{\mathcal{G}}\right]$$

$$\Pr\left[\mathsf{Game}^{EDL}_{\mathcal{H}',\mathcal{G},\mathcal{S}_1,\mathcal{F}}() : \mathsf{win}\right] \leq \Pr\left[\mathsf{Game}^{EDL}_{\mathcal{H}',\mathcal{G},\mathcal{S}_2,\mathcal{F}}() : \mathsf{win}\right] + \Pr\left[\mathsf{Game}^{EDL}_{\mathcal{H}',\mathcal{G},\mathcal{S}_1,\mathcal{F}}() : \mathsf{bad}_{\mathcal{G}}\right]$$

4) Reduction

For any forger $\mathcal{F}$, the forger's success probability either

- the forger solves its given CDH instance $(z = h^{sk})$ or
- the forger exploited the unsoundness in the proof of discrete logarithm equality $(z \neq h^{sk})$

$$\begin{aligned}\Pr\left[\mathsf{Game}^{\mathsf{EDL}}_{\mathcal{H}',\mathcal{G},\mathcal{S}_2,\mathcal{F}}() : \mathsf{win}\right] &= \Pr\left[\mathsf{Game}^{\mathsf{EDL}}_{\mathcal{H}',\mathcal{G},\mathcal{S}_2,\mathcal{F}}() : \mathsf{win} \wedge \tilde{\mathsf{z}} = \mathsf{h}^{\mathsf{sk}}\right] \\ &\quad + \Pr\left[\mathsf{Game}^{\mathsf{EDL}}_{\mathcal{H}',\mathcal{G},\mathcal{S}_2,\mathcal{F}}() : \mathsf{win} \wedge \tilde{\mathsf{z}} \neq \mathsf{h}^{\mathsf{sk}}\right]\end{aligned}$$

B. Chevallier-Mames(CM) -Crypto 2005

- Proposed a new signature scheme that also has a tight security reduction to CDH but whose resulting signatures are smaller than EDL signatures
- Message is not included in the random oracle query to $\mathcal{H}$ whose output serves as the second base for the proof of discrete logarithm equality

Summary

- First machine-checked proof for signature scheme based on discrete logarithm.
- We identify a proof schema that we believe applies more broadly.
- We refine some EasyCrypt techniques to reduce the proof burden and support better proof reuse. (Shim)