A Constructive Perspective on Signcryption Security

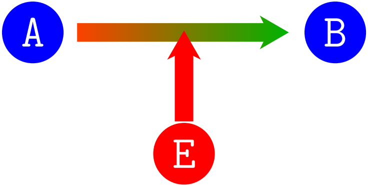
Christian Badertscher, Fabio Banfi, Ueli Maurer

ETH Zürich, Switzerland

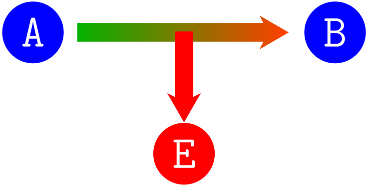
11th Conference on Security and Cryptography for Networks
September 5-7, 2018, Amalfi, Italy

Background: communication channels

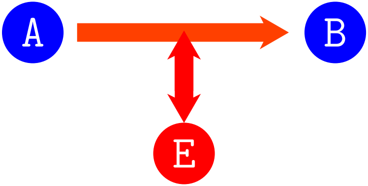
Confidential:



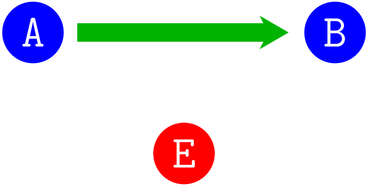
Authenticated:



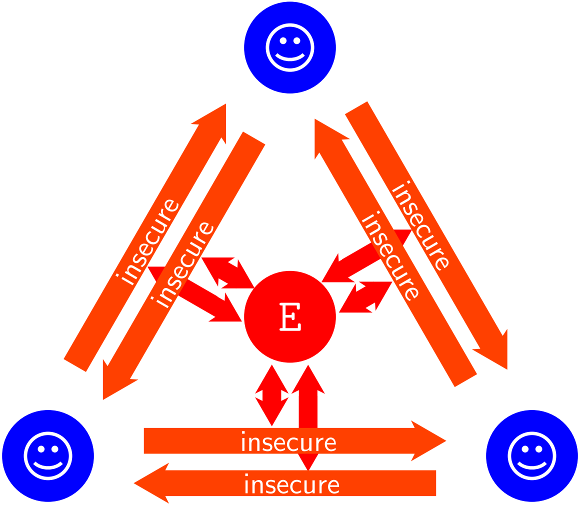
Insecure:



Secure:



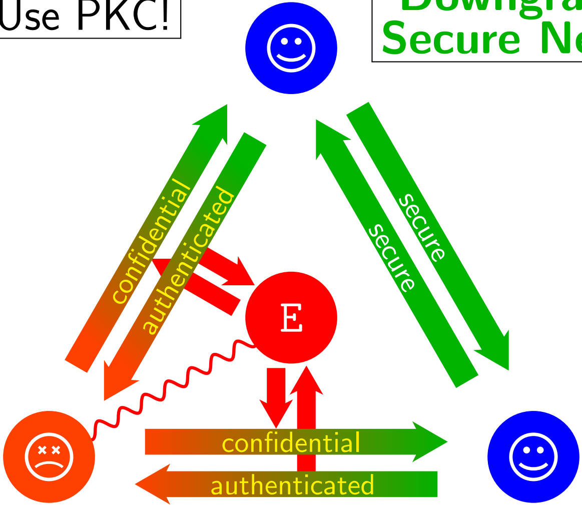
Our starting point: insecure network



Our goal: $\underbrace{\text{secure network with graceful degradation}}$

Downgradable Secure Network

$\Longrightarrow$ Use PKC!



Secret keys stolen?

Contribution

Question: What is the *right* security definition of signcryption?

Answer: The one for which a protocol using **signcryption** constructs

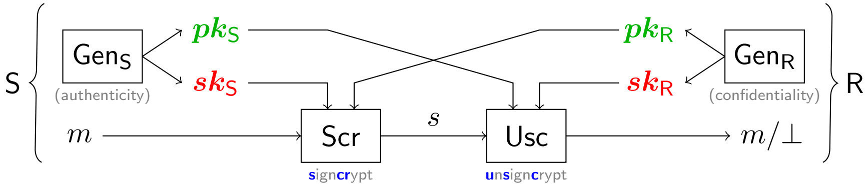
a **downgreadable secure network** from an **insecure network**

☞ We explain signcryption in a composable way to understand what it should be used for ☜

$\Longrightarrow$ For this we use the **Constructive Cryptography** framework

Signcryption: syntax

Signcryption ≈ encryption + signatures



Protocol:

- Users agree in advance on a scheme $\Psi \doteq (\mathsf{Gen_S}, \mathsf{Gen_R}, \mathsf{Scr}, \mathsf{Usc})$
- Each user generates sending and receiving key-pairs with Gen$_S$/Gen$_R$
- Each user publishes public keys through a *certificate authority*
- Each user sends/receives messages using Scr/Usc

Signcryption: security

Two game-based security definitions:

- **Outsider security:** the adversary is an outsider
  - Has no valid key-pairs
- **Insider security:** the adversary is a user of the network
  - Can have/generate valid key-pairs

In the games of both security definitions we have **flexible oracles**:

$\Longrightarrow$ Adversary can choose public keys of sending/receiving user

Signcryption: multi-user <u>outsider</u> security

New **<u>all-in-one</u>** security definition: $\underbrace{\text{confidentiality}}_{\text{CCA2}} + \underbrace{\text{authenticity}}_{\text{SUF}}$

Fix **sender** S with $(\boldsymbol{sk}_{\mathsf{S}}, \boldsymbol{pk}_{\mathsf{S}})$ and **receiver** R with $(\boldsymbol{sk}_{\mathsf{R}}, \boldsymbol{pk}_{\mathsf{R}})$

$$\left.\begin{matrix} \mathsf{Scr}_{\boldsymbol{sk}_{\mathsf{S}}}(\bullet,\bullet) \\ \mathsf{Usc}^{*}_{\boldsymbol{sk}_{\mathsf{R}}}(\bullet,\bullet) \end{matrix}\right\} \overset{b=1}{\longleftrightarrow} \quad \mathcal{A} \quad \overset{b=0}{\longleftrightarrow} \left\{\begin{matrix} \mathsf{Scr}^{\$}_{\boldsymbol{sk}_{\mathsf{S}}}(\bullet,\bullet) \\ \mathsf{Usc}^{\perp}_{\boldsymbol{sk}_{\mathsf{R}}}(\bullet,\bullet) \end{matrix}\right. \qquad \boxed{\Longrightarrow \mathbf{Adv}^{\mathsf{MOS}}_{\Psi,\mathcal{A}}}$$

$$\Downarrow$$

$$b' \quad (\overset{!}{=} b)$$

- $\mathsf{Usc}^{*}_{\boldsymbol{sk}_{\mathsf{R}}}(\bullet,\bullet)$: only unsigncrypt *new* signcryptexts if $\bullet = \boldsymbol{pk}_{\mathsf{S}}$ (return $\perp$)
- $\mathsf{Scr}^{\$}_{\boldsymbol{sk}_{\mathsf{S}}}(\bullet,\bullet)$: signcrypt random messages instead if $\bullet = \boldsymbol{pk}_{\mathsf{R}}$
- $\mathsf{Usc}^{\perp}_{\boldsymbol{sk}_{\mathsf{R}}}(\bullet,\bullet)$: always output $\perp$ if $\bullet = \boldsymbol{pk}_{\mathsf{S}}$

Signcryption: multi-user insider security

Confidentiality: fix **receiver** R with $(\textcolor{red}{\boldsymbol{sk}_{\mathsf{R}}}, \textcolor{green}{\boldsymbol{pk}_{\mathsf{R}}})$

$$\left.\begin{array}{l}\mathsf{Scr}((\textcolor{red}{\bullet},\textcolor{green}{\bullet}), \textcolor{green}{\bullet}, \bullet) \\ \mathsf{Usc}^*_{\textcolor{red}{\boldsymbol{sk}_{\mathsf{R}}}}(\textcolor{green}{\bullet}, \bullet)\end{array}\right\} \overset{b=1}{\longleftrightarrow} \quad \mathcal{A} \quad \overset{b=0}{\longleftrightarrow} \left\{\begin{array}{l}\mathsf{Scr}^{\$}((\textcolor{red}{\bullet},\textcolor{green}{\bullet}), \textcolor{green}{\bullet}, \bullet) \\ \mathsf{Usc}^*_{\textcolor{red}{\boldsymbol{sk}_{\mathsf{R}}}}(\textcolor{green}{\bullet}, \bullet)\end{array}\right.$$

$$\Downarrow$$

$$b' \quad (\overset{!}{=} b)$$

$$\boxed{\Longrightarrow \mathbf{Adv}^{\mathsf{MIS\text{-}Conf}}_{\Psi,\mathcal{A}}}$$

Authenticity: fix **sender** S with $(\textcolor{red}{\boldsymbol{sk}_{\mathsf{S}}}, \textcolor{green}{\boldsymbol{pk}_{\mathsf{S}}})$

$$\mathcal{A} \quad \longleftrightarrow \left\{\begin{array}{l}\mathsf{Scr}_{\textcolor{red}{\boldsymbol{sk}_{\mathsf{S}}}}(\textcolor{green}{\bullet}, \bullet) \\ \mathsf{Usc}((\textcolor{red}{\bullet},\textcolor{green}{\bullet}), \textcolor{green}{\bullet}, \bullet)\end{array}\right.$$

$$\Downarrow$$

s^* (**new** and **valid**)

$$\boxed{\Longrightarrow \mathbf{Adv}^{\mathsf{MIS\text{-}Auth}}_{\Psi,\mathcal{A}}}$$

The result

In **Constructive Cryptography**, our statement for n users is:

$$[\mathbf{ISN}_n, \mathbf{CA}_n, \mathbf{M}_n] \xRightarrow{(\boldsymbol{\pi}, \varepsilon)} \mathbf{DSN}_n$$

We construct a *Downgradable Secure Network* from an *Insecure Network*

with the help of *Signcryption*, a *Certificate Authority*, and some *Memory*

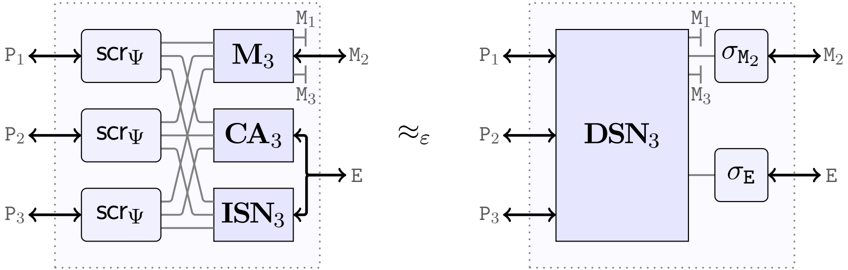
In particular, this means:

$$\forall\, \mathbf{D} : \exists \boldsymbol{\sigma} : \quad \Delta^{\mathbf{D}}(\boldsymbol{\pi}\, [\mathbf{ISN}_n, \mathbf{CA}_n, \mathbf{M}_n], \boldsymbol{\sigma}\, \mathbf{DSN}_n) \leq \varepsilon(\mathbf{D})$$

where $\varepsilon(\mathbf{D}) \doteq n^2 \cdot \mathbf{Adv}^{\mathsf{MOS}}_{\Psi,\, \rho_1(\mathbf{D})} + n \cdot \mathbf{Adv}^{\mathsf{MIS\text{-}Conf}}_{\Psi,\, \rho_2(\mathbf{D})} + n \cdot \mathbf{Adv}^{\mathsf{MIS\text{-}Auth}}_{\Psi,\, \rho_3(\mathbf{D})}$,

for efficient black-box *reductions* $\rho_1(\cdot)$, $\rho_2(\cdot)$, and $\rho_3(\cdot)$

Illustration for 3 users



Conclusions

- In the literature, **insider security** sometimes considered “too strong”
- In this work, we explained signcryption in a composable way
- Our analysis helped identifying the “right” security definition
  - **Outsider security** alone is limited, no security guarantees for key theft
  - **Insider security** enables exactly *“downgradable security”*

Thank you for your attention!