Anonymous Authenticated Communication

Fabio Banfi and Ueli Maurer

ETH Zurich, Switzerland

13th Conference on Security and Cryptography for Networks
September 12-14, 2022, Amalfi, Italy

Introduction

Anonymity vs. authenticity: two conflicting goals?

- **Anonymity:** the "identity" of the sender/receiver is *hidden*
- **Authenticity:** the "identity" of the sender is *known*

How can we study this problem **composably**?

We use the **constructive cryptography** (**CC**) framework:

- Resources (functionalities) with an interface for each user
- Identities modeled by the *labels* of the interfaces

Constructive Cryptography (CC)

Two main ingredients:

- **Resources:** $\mathbf{R} \in \Phi$ is a *discrete system* with interfaces $I \in \mathcal{I}$
  - E.g.: $S_1, \ldots, S_n$ for the *senders*, R for the *receiver*, E for the *adversary*
  - **Parallel composition:** for $\mathbf{R}, \mathbf{S} \in \Phi$: $[\mathbf{R}, \mathbf{S}] \in \Phi$ (*sub-interfaces*)
- **Converters:** *discrete system* α s.t. $\alpha^I \mathbf{R} \in \Phi$, for interface $I \in \mathcal{I}$
  - **Protocol:** E.g., $\pi = (\alpha^{S_1}, \ldots, \alpha^{S_n}, \beta^R)$

Construction: $\mathbf{R} \overset{\pi}{\Longrightarrow} \mathbf{S} \iff \exists$ simulator σ: $\pi\mathbf{R} \approx \sigma^E \mathbf{S}$

Composition: $\mathbf{R} \overset{\pi}{\Longrightarrow} \mathbf{S} \ \wedge \ \mathbf{S} \overset{\phi}{\Longrightarrow} \mathbf{T} \implies \mathbf{R} \overset{\phi \circ \pi}{\Longrightarrow} \mathbf{T}$

Anonymous Communication Channels

Four common communication channels (CC resources):

- **Insecure (INS):** adversary can *eavesdrop* and *inject*
- **Authenticated (AUT):** adversary can only *eavesdrop* (**not** *inject*)
- **Confidential (CNF):** adversary can only *inject* (**not** *eavesdrop*)
- **Secure (SEC):** authenticated + confidential

n senders, 1 receiver			1 sender, n receivers		
Symbol	**Leaked**	**Inject**	**Symbol**	**Leaked**	**Inject**
A-INS$_{n\to 1}$	~~$\mathcal{P}_i$~~, m	✓	A-INS$_{1\to n}$	~~P_i~~, m	✓
A-AUT$_{n\to 1}$	~~$\mathcal{P}_i$~~, m	✗	A-AUT$_{1\to n}$	~~P_i~~, m	✗
A-CNF$_{n\to 1}$	~~$\mathcal{P}_i$~~, $\lvert m\rvert$	✓	A-CNF$_{1\to n}$	~~P_i~~, $\lvert m\rvert$	✓
A-SEC$_{n\to 1}$	~~$\mathcal{P}_i$~~, $\lvert m\rvert$	✗	A-SEC$_{1\to n}$	~~P_i~~, $\lvert m\rvert$	✗

$\Longrightarrow$ We are considering **preservation** of *(external)* anonymity

Related Work

- [AHM+15]: $[\underbrace{\text{KEY}_{n\leftrightarrow 1}}_{1\leftrightarrow n}, \underbrace{\textbf{A-INS}_{n\to 1}}_{1\to n}] \overset{\pi_{\text{pMAC}}}{\Longmapsto} \underbrace{\textbf{A-AUT}_{n\to 1}}_{1\to n}$
- [BM20]: $[\underbrace{\text{KEY}_{n\leftrightarrow 1}}_{1\leftrightarrow n}, \overbrace{\underbrace{\textbf{A-AUT}_{n\to 1}}_{1\to n}}^{\textbf{A-INS}_{n\to 1}}] \overset{\overbrace{\pi_{\text{pE}}}^{\pi_{\text{pAE}}}}{\Longmapsto} \underbrace{\textbf{A-SEC}_{n\to 1}}_{1\to n}$
- [KMO+13]: $[\text{1-AUT}_{1\leftarrow n}, \textbf{A-INS}_{1\to n}] \overset{\pi_{\text{PKE}}}{\Longmapsto} \textbf{A-CNF}_{1\to n}$

	Sender anonymity	Receiver anonymity
Symmetric	[AHM+15, BM20]	[AHM+15, BM20]
Asymmetric	**This work**	[KMO+13]

$\Longrightarrow$ Intuitively, *signatures* should be used here!

Anonymous Signatures?

Consider a *probabilistic* signature scheme $\Sigma \doteq (\texttt{Gen}, \texttt{Sgn}, \texttt{Vrf})$

How could we define anonymity? **Key-indistinguishability (IK)**

Given pk_1 and pk_2, provide m and then distinguish between:

- (σ_1, σ_2), where $\sigma_i \leftarrow \texttt{Sgn}_{sk_i}(m)$
- (σ_1, σ_2), where $\sigma_i \leftarrow \texttt{Sgn}_{sk_I}(m)$, for $I \xleftarrow{\$} [2]$

Does it work? **NO:** we can simply use $\texttt{Vrf}$ with pk_1, pk_2 to distinguish!

In fact, we show: for any protocol π,

$$[\text{1-AUT}_{n\to 1}, \textbf{A-INS}_{n\to 1}] \overset{\pi}{\not\Longrightarrow} \textbf{A-AUT}_{n\to 1}$$

$\Longrightarrow$ We need to modify the syntax of Σ!

Possible Workarounds

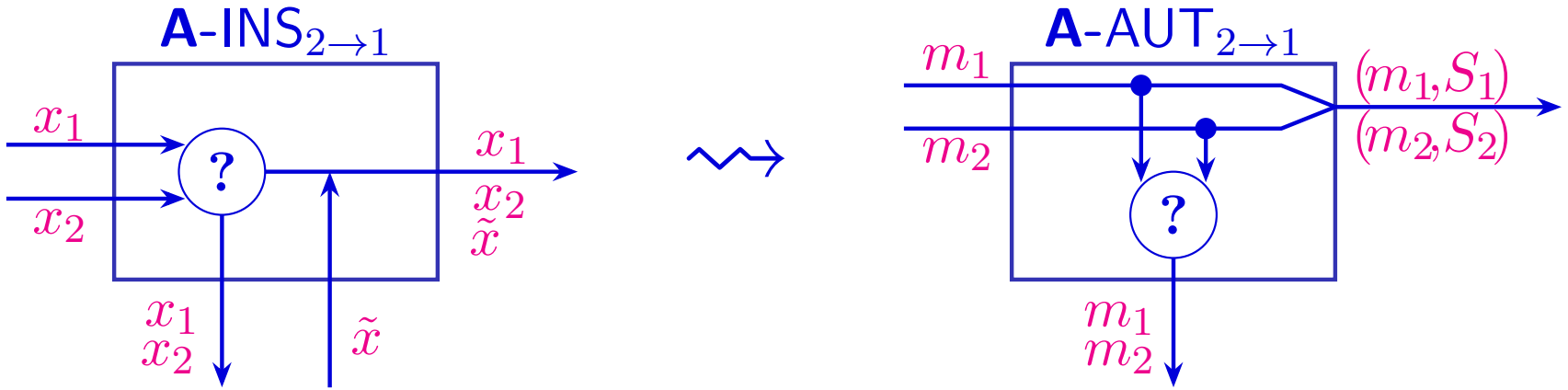
We identify three axis along which we functionally relax the construction

1. Change the *assumed* resource:
   - $[\text{1-AUT}_{n\leftarrow 1}, \text{1-AUT}_{n\rightarrow 1}, \textbf{A}\text{-INS}_{n\rightarrow 1}] \overset{\pi_{\text{BS}}}{\Longmapsto} \textbf{A}\text{-AUT}_{n\rightarrow 1}$
   - **Anonymous authentication:** use *bilateral signatures* (new)
2. Change the *constructed* resource:
   - $[\text{1-AUT}_{n\rightarrow 1}, \textbf{A}\text{-INS}_{n\rightarrow 1}] \overset{\pi_{\text{PS}}}{\Longmapsto} \textbf{D}\text{-AUT}_{n\rightarrow 1}$
   - **De-anonymizable authentication:** use *partial signatures* [BD09]
3. Change *both* resources:
   - $[\text{1-AUT}_{n\circlearrowleft 1}, \textbf{A}\text{-INS}_{n\rightarrow 1}] \overset{\pi_{\text{RS}}}{\Longmapsto} \textbf{RA}\text{-AUT}_{n\rightarrow 1}$
   - **Receiver-side anonymous authentication:** use *ring signatures* [BKM06]

1. Anonymous Authentication

First approach:

- Change the assumed res.: $\mathbf{R} \doteq [1\text{-AUT}_{n\leftarrow 1}, 1\text{-AUT}_{n\rightarrow 1}, \mathbf{A}\text{-INS}_{n\rightarrow 1}]$
- Keep the constructed resource: $\mathbf{S} \doteq \mathbf{A}\text{-AUT}_{n\rightarrow 1}$



$\Longrightarrow$ We preserve anonymity towards an *eavesdropper*

Bilateral Signatures

Idea: make verification require a *secret from the receiver*!

π_{BS} uses scheme $\Sigma_{\mathsf{BS}} \doteq (\mathtt{Gen}_S, \mathtt{Gen}_R, \mathtt{Sgn}, \mathtt{Vrf})$ as follows:

- Setup:
  - Sender S_i gets $(ssk_i, spk_i) \leftarrow \mathtt{Gen}_S$ and sends spk_i over $\text{1-AUT}_{n\to 1}$
  - Receiver R gets $(rsk, rpk) \leftarrow \mathtt{Gen}_R$ and sends rpk over $\text{1-AUT}_{n\leftarrow 1}$
- Communication:
  - S_i sends (m, σ) over $\textbf{A-INS}_{n\to 1}$, where $\sigma \leftarrow \mathtt{Sgn}_{ssk_i, rpk}(m)$
  - R gets $v_i = \mathtt{Vrf}_{rsk, spk_i}(m, \sigma)$ for all i and outputs (m, S_i) iff $v_i = 1$

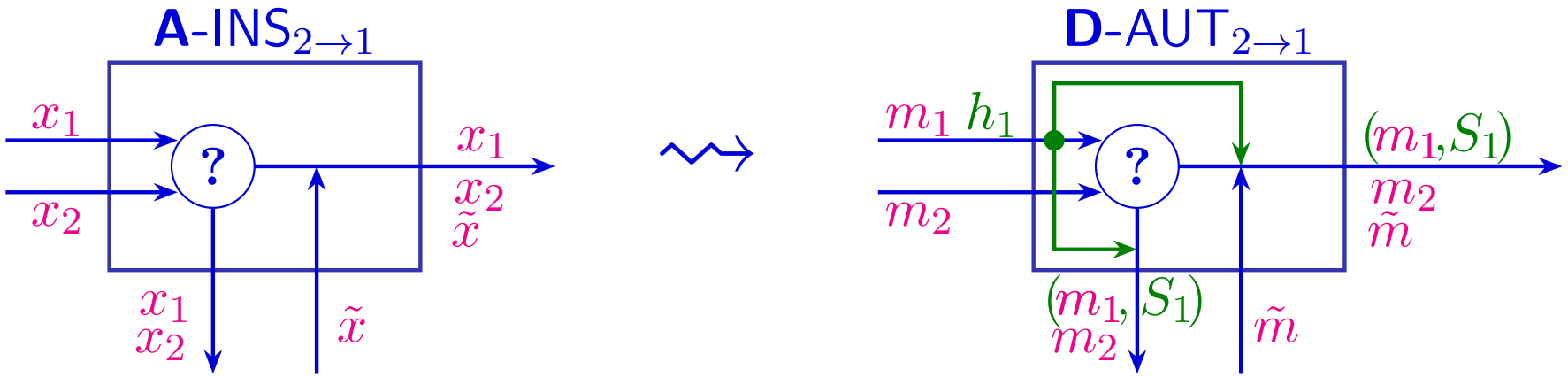
We show: if Σ_{BS} is UF (auth.) and IK (anon.) secure, then

$$[\text{1-AUT}_{n\leftarrow 1}, \text{1-AUT}_{n\to 1}, \textbf{A-INS}_{n\to 1}] \overset{\pi_{\mathsf{BS}}}{\Longmapsto} \textbf{A-AUT}_{n\to 1}$$

2. De-Anonymizalbe Authentication

Second approach:

- Change the constructed resource: $\mathbf{S} \doteq \textbf{D-AUT}_{n\to 1}$
- Keep the assumed resource: $\mathbf{R} \doteq [\text{1-AUT}_{n\to 1}, \textbf{A-INS}_{n\to 1}]$



$\Longrightarrow$ *Selective* anonymity towards *eavesdropper and receiver*

Partial Signatures

Idea: split signatures into *anonymous* **stub** σ and *authenticating* **tag** τ!

$\implies$ σ anon. but *not authentic*, (σ, τ) auth. but *not anonymous*

π_{PS} uses scheme $\Sigma_{\mathsf{PS}} \doteq (\mathtt{Gen}, \mathtt{Sgn}, \mathtt{Vrf})$ as follows:

- Setup: sender S_i gets $(sk_i, pk_i) \leftarrow \mathtt{Gen}$ and sends pk_i over $\text{1-AUT}_{n\to 1}$
- Communication:
  1. Committing to m:
     - S_i sends (m, σ) over $\textbf{A-INS}_{n\to 1}$, where $(\sigma, \tau) \leftarrow \mathtt{Sgn}_{sk_i}(m)$
     - R outputs m, but could be from any S_i or adversary (can't use $\mathtt{Vrf}$)
  2. De-anonymizing m:
     - S_i sends (m, σ, τ) over $\textbf{A-INS}_{n\to 1}$
     - R gets $v_i = \mathtt{Vrf}_{pk_i}(m, \sigma, \tau)$ for all i and outputs (m, S_i) iff $v_i = 1$

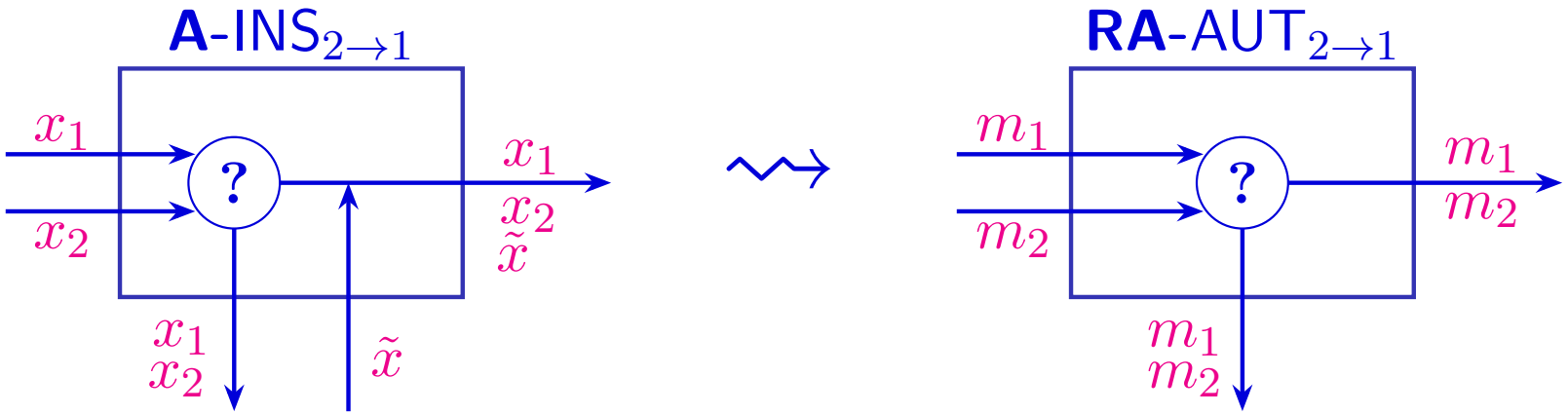
We show: if Σ_{PS} is UF (auth.), IK (anon.), UA (unamb.) secure, then

$$[\text{1-AUT}_{n\to 1}, \textbf{A-INS}_{n\to 1}] \overset{\pi_{\mathsf{PS}}}{\Longrightarrow} \textbf{D-AUT}_{n\to 1}$$

3. Receiver-Side Anonymous Authentication

Third approach:

- Change the assumed resource: $\mathbf{R} \doteq [\text{1-AUT}_{n\circlearrowleft 1}, \textbf{A-INS}_{n\to 1}]$
- Change the constructed resource: $\mathbf{S} \doteq \textbf{RA-AUT}_{n\to 1}$



$\Longrightarrow$ Anonymity towards both *eavesdropper and receiver*

Ring Signatures

Idea: make signatures depend on a *group of senders*!

π_{RS} uses scheme $\Sigma_{\mathsf{RS}} \doteq (\mathtt{Gen}, \mathtt{Sgn}, \mathtt{Vrf})$ as follows:

- Setup:
  - Sender S_i gets $(sk_i, pk_i) \leftarrow \mathtt{Gen}$ and sends pk_i over $\text{1-AUT}_{n\circlearrowleft 1}$
  - Each S_i and R set $\boldsymbol{pk} \doteq (pk_1, \ldots, pk_n)$
- Communication:
  - S_i sends (m, σ) over $\textbf{A-INS}_{n\to 1}$, where $\sigma \leftarrow \mathtt{Sgn}_{i,sk_i,\boldsymbol{pk}}(m)$
  - R gets $v = \mathtt{Vrf}_{\boldsymbol{pk}}(m, \sigma)$ and outputs m iff $v = 1$

We show: if Σ_{RS} is UF (auth.) and IK (anon.) secure, then

$$[\text{1-AUT}_{n\circlearrowleft 1}, \text{1-AUT}_{n\to 1}, \textbf{A-INS}_{n\to 1}] \overset{\pi_{\mathsf{RS}}}{\Longrightarrow} \textbf{RA-AUT}_{n\to 1}$$

Conclusions

- We filled a gap in the composable treatment of anonymity
  - Not as "straightforward" as in previous works
    - Multiple possible solutions (are there more?)
    - In one we incurred the simulator commitment "problem"

      $\Longrightarrow$ Solved using the recent technique of "interval-wise relaxations" [JM20]
- Future work:
  - Adaptive security?
  - Anonymity *creation* (rather than preservation)?
    - E.g, **A**-SEC$_{n\to 1}$ from from INS$_{n\to 1}$ using mix-nets/onion routing

Thank you for your attention!

References

Joël Alwen, Martin Hirt, Ueli Maurer, Arpita Patra, and Pavel Raykov.

Anonymous authentication with shared secrets.
In Diego F. Aranha and Alfred Menezes, editors, *LATINCRYPT 2014*, volume 8895 of *LNCS*, pages 219–236, Cham, 2015. Springer.

Mihir Bellare and Shanshan Duan.

Partial signatures and their applications.
Cryptology ePrint Archive, Report 2009/336, 2009.
https://eprint.iacr.org/2009/336.

Adam Bender, Jonathan Katz, and Ruggero Morselli.

Ring signatures: Stronger definitions, and constructions without random oracles.
In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 60–79, Heidelberg, 2006. Springer.

Fabio Banfi and Ueli Maurer.

Anonymous symmetric-key communication.
In Clemente Galdi and Vladimir Kolesnikov, editors, *SCN 2020*, volume 12238 of *LNCS*, pages 471–491, Cham, 2020. Springer.

Daniel Jost and Ueli Maurer.

Overcoming impossibility results in composable security using interval-wise guarantees.
In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020*, volume 12170 of *LNCS*, pages 33–62, Cham, 2020. Springer.

Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Björn Tackmann, and Daniele Venturi.

Anonymity-preserving public-key encryption: A constructive approach.
In Emiliano De Cristofaro and Matthew Wright, editors, *PETS 2013*, volume 7981 of *LNCS*, pages 19–39, Heidelberg, 2013. Springer.