Anonymous Symmetric-Key Communication

Fabio Banfi and Ueli Maurer

ETH Zurich, Switzerland

12th Conference on Security and Cryptography for Networks
September 14-16, 2020, Amalfi, Italy (Virtual)

Background: Schemes

We study **probabilistic** encryption (pE) / authenticated encryption (pAE):

$\Pi \doteq (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ where:

- $\mathtt{Gen}$ is a (usually uniform) distribution over $\mathcal{K}$;
- $\mathtt{Enc} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ is a *probabilistic* function;
- $\mathtt{Dec} : \mathcal{K} \times \mathcal{C} \to \mathcal{M} \cup \{\perp\}$ is a deterministic function.

In particular: we do *not* consider nonce-based schemes (nE/nAE)

Background: Probabilistic vs Nonce-based

Why study anonymity of pE/pAE rather than nE/nAE?

- [CR19] recently studied anonymity of nAE
  - nAE cannot provide anonymity $\implies$ New complex scheme: anAE
- pE/pAE conceptually easier and more suitable for anonymity
- Also closely captures some real-world implementations:
  - Consider nAE scheme AES-GCM deployed in TLS 1.3:
  - Uses **randomized nonces** $\implies$ This reduces nAE to pAE!

Background: Security

Conventional security notions for pE/pAE:

- pE: should achieve **confidentiality**
- pAE: should achieve **confidentiality** and **authenticity**

How is security defined?

- **Game-based**: adversary must win a game (bit-guessing/search)
  - Can be formulated as a distinction problem
- **Composable**: simulation-based, distinguish real/ideal worlds

$\Longrightarrow$ We will see how the two are actually closely related

Background: Cryptographic Systems

For security definitions, we define following systems for $K \leftarrow \texttt{Gen}()$:

- $\mathbf{E}_K$: on input m, output $\texttt{Enc}_K(m)$,
- $\mathbf{D}_K$: on input c, output $\texttt{Dec}_K(c)$,
- $\mathbf{E}_K^{\$}$: on input m, output $\texttt{Enc}_K(\tilde{m})$ for $\tilde{m} \stackrel{\$}{\leftarrow} \{0,1\}^{|m|}$
- $\mathbf{D}^{\perp}$: on input c, output $\perp$
- $\mathbf{\$}$: on input m, output $\tilde{c}$ for $\tilde{c} \stackrel{\$}{\leftarrow} \{0,1\}^{|\texttt{Enc}_K(m)|}$

$\mathbf{S} \approx \mathbf{T}$: systems $\mathbf{S}$ and $\mathbf{T}$ are **computationally indistinguishable**

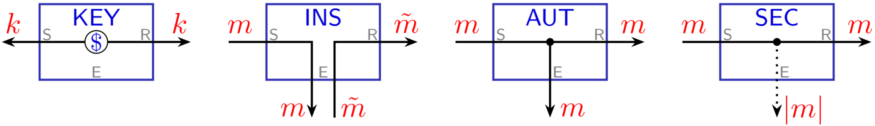
Background: Game-based Security of pE/pAE

- pE: IND-CPA
  - Usually a bit-guessing problem
  - Here a distinction problem [BDJR97]: $\mathbf{E}_K \approx \mathbf{E}_K^{\$}$
- pAE: IND-CPA + INT-CTXT = IND-CCA3
  - Usually a bit-guessing problem + search problem
  - Here a distinction problem [Shr04]: $[\mathbf{E}_K, \mathbf{D}_K] \approx [\mathbf{E}_K^{\$}, \mathbf{D}^{\perp}]$

$\Longrightarrow$ Implicit assumption: 1 sender (S), 1 receiver (R), 1 eavesdropper (E)

Background: Composable Security of pE/pAE

Resources for sender S, receiver R, and eavesdropper E:



Using **constructive cryptography**, we define:

- pE secure if constructs SEC from AUT and KEY:

$$[\mathsf{KEY}, \mathsf{AUT}] \xrightarrow{\mathsf{pE}} \mathsf{SEC} \quad :\Longleftrightarrow \quad \exists \mathsf{sim} : \mathsf{pE}([\mathsf{KEY}, \mathsf{AUT}]) \approx \mathsf{sim}(\mathsf{SEC})$$

- pAE secure if constructs SEC from INS and KEY:

$$[\mathsf{KEY}, \mathsf{INS}] \xrightarrow{\mathsf{pAE}} \mathsf{SEC} \quad :\Longleftrightarrow \quad \exists \mathsf{sim} : \mathsf{pAE}([\mathsf{KEY}, \mathsf{INS}]) \approx \mathsf{sim}(\mathsf{SEC})$$

Background: Game-based $\Longrightarrow$ Composable

How do these definitions relate?

- pE IND-CPA-secure $\Longrightarrow$ $[\mathsf{KEY}, \mathsf{AUT}] \xrightarrow{\mathsf{pE}} \mathsf{SEC}$, i.e.:

  $$\mathbf{E}_K \approx \mathbf{E}_K^{\$} \Longrightarrow \exists \mathsf{sim} : \mathsf{pE}([\mathsf{KEY}, \mathsf{AUT}]) \approx \mathsf{sim}(\mathsf{SEC})$$

- pAE IND-CCA3-secure $\Longrightarrow$ $[\mathsf{KEY}, \mathsf{INS}] \xrightarrow{\mathsf{pAE}} \mathsf{SEC}$, i.e.:

  $$[\mathbf{E}_K, \mathbf{D}_K] \approx [\mathbf{E}_K^{\$}, \mathbf{D}^{\perp}] \Longrightarrow \exists \mathsf{sim} : \mathsf{pAE}([\mathsf{KEY}, \mathsf{INS}]) \approx \mathsf{sim}(\mathsf{SEC})$$

Game-based Anonymity: New Definitions

BUT: Real-world usage of pE/pAE happens in a **multi-user** setting!

$\implies$ We consider n $(= 2)$ senders ($+$ 1 receiver, 1 eavesdropper)

Anonymity modeled by **indistinguishability of keys** (IK):

- pE: IND-CPA $+$ IK-CPA $=$ IND-IK-CPA if

$$[\mathbf{E}_{K_1}, \mathbf{E}_{K_2}] \approx [\mathbf{E}^{\$}_{K}, \mathbf{E}^{\$}_{K}]$$

- pAE: IND-CCA3 $+$ IK-CCA3 $=$ IND-IK-CCA3 if

$$[\mathbf{E}_{K_1}, \mathbf{D}_{K_1}, \mathbf{E}_{K_2}, \mathbf{D}_{K_2}] \approx [\mathbf{E}^{\$}_{K}, \mathbf{D}^{\perp}, \mathbf{E}^{\$}_{K}, \mathbf{D}^{\perp}]$$

Game-based Anonymity: IND\$ and Enc-then-MAC

- IND\$-{CPA,CCA3} implies anonymity (IND-IK-{CPA,CCA3}):
  - pE: $\mathbf{E}_K \approx \mathbf{\$} \implies [\mathbf{E}_{K_1}, \mathbf{E}_{K_2}] \approx [\mathbf{E}^{\$}_K, \mathbf{E}^{\$}_K]$
  - pAE: $[\mathbf{E}_K, \mathbf{D}_K] \approx [\mathbf{\$}, \mathbf{D}^{\perp}]$

$$\implies [\mathbf{E}_{K_1}, \mathbf{D}_{K_1}, \mathbf{E}_{K_2}, \mathbf{D}_{K_2}] \approx [\mathbf{E}^{\$}_K, \mathbf{D}^{\perp}, \mathbf{E}^{\$}_K, \mathbf{D}^{\perp}]$$

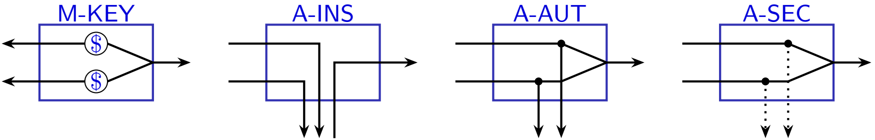
  Note: IND\$-secure nAE with randomized nonces provides anonymity!

- Encrypt-then-MAC is **anonymity-preserving**:

  If pE is IND-IK-CPA-secure and pMAC is UF-IK-CMA-secure

  $\implies$ pAE := EtM(pE,pMAC) is IND-IK-CCA3-secure

Composable Anonymity: Adapting the Resources



[AHM+14]: UF-IK-CMA-secure pMAC constructs

- A-AUT from A-INS and M-KEY
- A-SEC from A-AUT **(inefficient)**
- A-SEC from A-INS and from M-KEY **(inefficient)**

Composable Anonymity: New Definitions

We use again **constructive cryptography** to define anonymous security:

- pE secure **and anon.** if constructs A-SEC from A-AUT and M-KEY:

  $$[\text{M-KEY}, \text{A-AUT}] \xrightarrow{\text{pE}} \text{A-SEC}$$

  $$:\Longleftrightarrow \quad \exists \text{sim} : \text{pE}([\text{M-KEY}, \text{A-AUT}]) \approx \text{sim}(\text{A-SEC})$$

- pAE secure **and anon.** if constructs A-SEC from A-INS and M-KEY:

  $$[\text{M-KEY}, \text{A-INS}] \xrightarrow{\text{pAE}} \text{A-SEC}$$

  $$:\Longleftrightarrow \quad \exists \text{sim} : \text{pAE}([\text{M-KEY}, \text{A-INS}]) \approx \text{sim}(\text{A-SEC})$$

Game-based Anon. $\Longrightarrow$ Composable Anon.

How do these definitions relate?

- pE IND-IK-CPA-secure $\Longrightarrow$ $[\text{M-KEY}, \text{A-AUT}] \xrightarrow{\text{pE}} \text{A-SEC}$, i.e.:

  $$[\mathbf{E}_{K_1}, \mathbf{E}_{K_2}] \approx [\mathbf{E}^{\$}_{K}, \mathbf{E}^{\$}_{K}]$$

  $$\Longrightarrow \exists \text{sim} : \text{pE}([\text{M-KEY}, \text{A-AUT}]) \approx \text{sim}(\text{A-SEC})$$

- pAE IND-IK-CCA3-secure $\Longrightarrow$ $[\text{M-KEY}, \text{A-INS}] \xrightarrow{\text{pAE}} \text{A-SEC}$, i.e.:

  $$[\mathbf{E}_{K_1}, \mathbf{D}_{K_1}, \mathbf{E}_{K_2}, \mathbf{D}_{K_2}] \approx [\mathbf{E}^{\$}_{K}, \mathbf{D}^{\perp}, \mathbf{E}^{\$}_{K}, \mathbf{D}^{\perp}]$$

  $$\Longrightarrow \exists \text{sim} : \text{pAE}([\text{M-KEY}, \text{A-INS}]) \approx \text{sim}(\text{A-SEC})$$

Conclusions

- We provided game-based anonymity definitions for pE/pAE:
  - Pseudorandom ciphertexts (IND$) imply anonymity

    $\Longrightarrow$ nAE with randomized nonces provides anonymity
  - Enc-then-MAC **preserves anonymity**
- We also provided **composable** anonymity definitions for pE/pAE:
  - They provide a better understanding of the application
  - They are implied by the game-based definitions
  - They allow for more efficient protocols than known before

Thank you for your attention!

References

- Joël Alwen, Martin Hirt, Ueli Maurer, Arpita Patra, and Pavel Raykov, *Anonymous authentication with shared secrets*, LATINCRYPT, 2014.
- M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, *A concrete security treatment of symmetric encryption*, FOCS, 1997.
- John Chan and Phillip Rogaway, *Anonymous AE*, ASIACRYPT, 2019.
- Tom Shrimpton, *A characterization of authenticated-encryption as a form of chosen-ciphertext security*, Cryptology ePrint Archive, 2004.