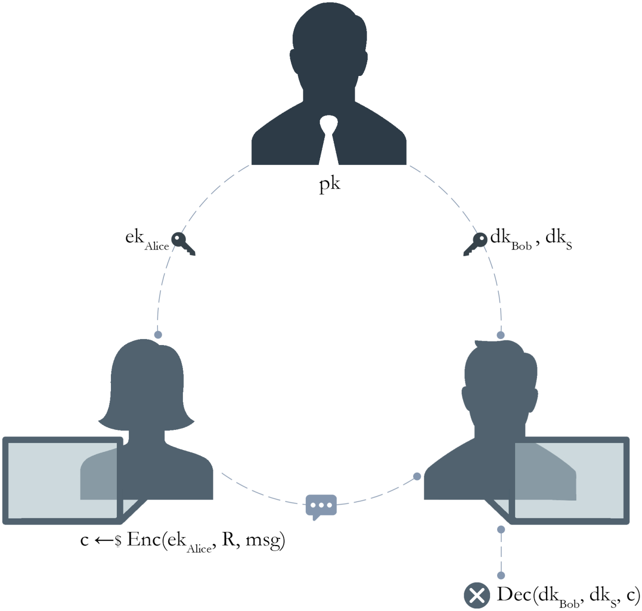
Matchmaking Encryption against Chosen-Ciphertext Attacks

Luigi Russo

September 27, 2020

Matchmaking Encryption 101



General Setting

- Key Generation, managed by the trusted party:
  - $\mathsf{SKGen}(\mathsf{msk}, \sigma)$
  - $\mathsf{RKGen}(\mathsf{msk}, \rho)$
  - $\mathsf{PolGen}(\mathsf{msk}, \mathsf{S})$
- Encryption. $\mathsf{Enc}(\mathsf{ek}_\sigma, \mathsf{R}, \mathsf{m})$
- Decryption. $\mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{dk}_\mathsf{S}, \mathsf{c})$
- Correctness. If $\mathsf{S}(\sigma) = \mathsf{R}(\rho) = 1:$

$$\Pr[\mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{dk}_\mathsf{S}, \mathsf{Enc}(\mathsf{ek}_\sigma, \mathsf{R}, \mathsf{m})) = 1] \geqslant 1 - \mathsf{negl}(\lambda)$$

Arranged Matchmaking

- Key Generation, managed by the trusted party:
  - $\mathsf{SKGen}(msk, \sigma)$
  - $\mathsf{RKGen}(msk, \rho, \mathbb{S})$
  - ~~$\mathsf{PolGen}(msk, \mathbb{S})$~~
- Encryption: $\mathsf{Enc}(ek_\sigma, \mathbb{R}, m)$
- Decryption: $\mathsf{Dec}(dk_{\rho,\mathbb{S}}, c)$
- Correctness. If $\mathbb{S}(\sigma) = \mathbb{R}(\rho) = 1$:

$$\Pr[\mathsf{Dec}(dk_{\rho,\mathbb{S}}, \mathsf{Enc}(ek_\sigma, \mathbb{R}, m)) = 1] \geqslant 1 - \mathsf{negl}(\lambda)$$

Signature Schemes

A signature scheme $\Pi = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Ver})$ satisfies:

1. **Correctness.** $\forall \lambda \in \mathbb{N}$, $\forall (sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$, and $\forall m \in \mathcal{M}$:

$$P[\mathsf{Ver}(pk, m, \mathsf{Sign}(sk, m)) = 1] = 1.$$

2. **EUF-CMA.** $\forall$ PPT $\mathcal{A}$:

$$\Pr[G^{euf}_{\Pi,\mathcal{A}}(\lambda) = 1] \leqslant \mathsf{negl}(\lambda)$$

where $G^{euf}_{\Pi,\mathcal{A}}(\lambda)$ is the following game:

- $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$.
- $(m, s) \leftarrow \mathcal{A}^{\mathsf{Sign}(sk,\cdot)}(1^\lambda, pk)$
- If $m \notin \mathcal{Q}_{\mathsf{Sign}}$, and $\mathsf{Ver}(pk, m, s) = 1$, output 1, else 0.

Non-Interactive Zero-Knowledge

A NIZK proof system $\Pi = (\mathsf{Gen}, \mathsf{P}, \mathsf{V})$ for a relation R satisfies:

1. **Completeness.** $\forall y \in \mathsf{L}$:

$$\Pr[\mathsf{V}(\omega, y, \pi) = 1 : \omega \leftarrow \mathsf{Gen}(1^\lambda), \pi \leftarrow \mathsf{P}(\omega, y, x)] = 1$$

2. **Soundness.** $\forall y \notin \mathsf{L}, \forall \mathsf{P}^*$:

$$\Pr[\mathsf{V}(\omega, y, \pi) = 1 : \omega \leftarrow \mathsf{Gen}(1^\lambda), \pi \leftarrow \mathsf{P}^*(\omega, y)] \in \mathsf{negl}(\lambda)$$

3. **Zero-Knowledge.** $\exists (\mathsf{Z}_0, \mathsf{Z}_1)$ s.t. $\forall y \in \mathsf{L}$:

$$\{\omega, \mathsf{Z}_1(\zeta, y) : (\omega, \zeta) \leftarrow \mathsf{Z}_0(1^\lambda)\}$$

$$\approx_c$$

$$\{\omega, \mathsf{P}(\omega, y, x) : \omega \leftarrow \mathsf{Gen}(1^\lambda)\}$$

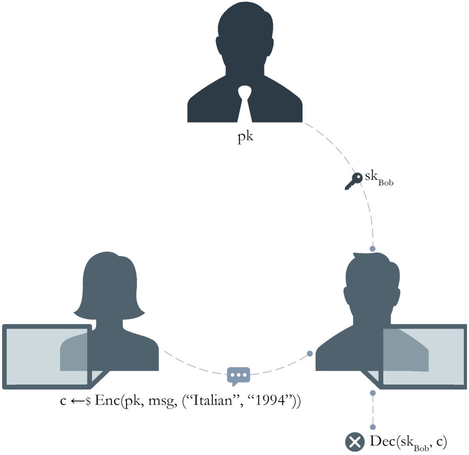
True-Simulation Extractability

A NIZK Π for a relation R satisfies true-simulation f-extractability for a function f if $\exists$ PPT extractor $K = (K_0, K_1)$ s. t. $\forall \mathcal{A}$:

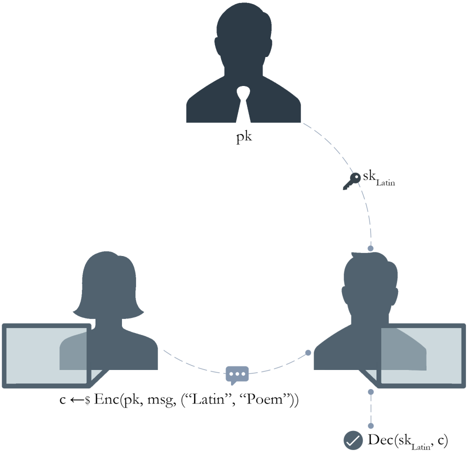
$$\Pr\left[\begin{array}{c} \mathsf{Ver}(\omega, y, \pi) = 1 \wedge \\ (y, \pi) \notin \mathcal{O}_O \wedge \\ \forall x : f(x) = z, (y, x) \notin R \end{array} : \begin{array}{c} (\omega, \zeta, \xi) \leftarrow K_0(1^\lambda) \wedge \\ (y, \pi) \leftarrow \mathcal{A}^{O(\zeta,(\cdot,\cdot))}(\omega) \wedge \\ z \leftarrow K_1(\xi, y, \pi) \end{array}\right]$$

* the oracle $O(\zeta, \cdot, \cdot)$ takes as input a pair (y, x) and returns $Z_1(\zeta, y)$ if $(y, x) \in R$ (and otherwise $\perp$).

Attribute-Based Encryption



Ciphertext-Policy ABE



Key-Policy ABE

CCA Privacy

Captures secrecy of sender's inputs.

$\underline{G^{priv}_{\Pi,A}(\lambda, b)}$:

$$
\begin{aligned}
&(\mathsf{mpk}, \mathsf{kpol}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda) \\
&(m_0, m_1, R_0, R_1, \sigma_0, \sigma_1, \alpha) \leftarrow A_1^{O_1, O_2, O_3, O_4}(1^\lambda, \mathsf{mpk}) \\
&\mathsf{ek}_{\sigma_b} \leftarrow \mathsf{SKGen}(\mathsf{msk}, \sigma_b) \\
&c \leftarrow \mathsf{Enc}(\mathsf{ek}_{\sigma_b}, R_b, m_b) \\
&b' \leftarrow A_2^{O_1, O_2, O_3, O_4}(1^\lambda, c, \alpha)
\end{aligned}
$$

CCA Authenticity

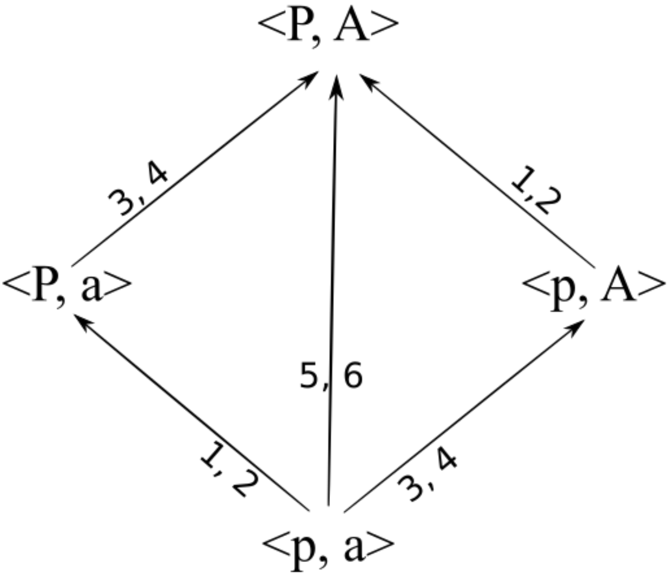
Captures security against malicious senders.

$\underline{G^{auth}_{\Pi,A}(\lambda)}$:

$$(mpk, kpol, msk) \leftarrow Setup(1^\lambda)$$
$$(c, \rho, S) \leftarrow A_1^{O_1, O_2, O_3, O_5}(1^\lambda, mpk)$$
$$dk_\rho \leftarrow RKGen(msk, \rho_b)$$
$$dk_S \leftarrow PolGen(kpol, S)$$
$$m = Dec(dk_\rho, dk_S, c)$$

$$(c \notin O_{O_5}) \wedge \forall \sigma \in \mathcal{Q}_{O_1} : (S(\sigma) = 0) \wedge (m \neq \perp)$$

CCA Transformation Lattice



Showcase: CCA Direct Transformation

To encrypt message m under sender attributes σ and policy R:

1. encrypt m using the underlying ME scheme
2. add a NIZK argument of the knowledge of m and a valid* signature s on σ.

* produced by a trusted party.

Sketch Proof

- CCA-authenticity reduced to EUF-CMA.
- CCA-privacy reduced to CPA-Privacy: the decryption oracle is simulated thanks to true-simulation f-extractability of the NIZK. We assume $f(\sigma, s, R, m, r) = (\sigma, s, R, m)$.

Open problems

- ME from standard assumptions
- Efficient IB-ME constructions
- Mitigating Key Escrow
- Blackbox Constructions from ABE