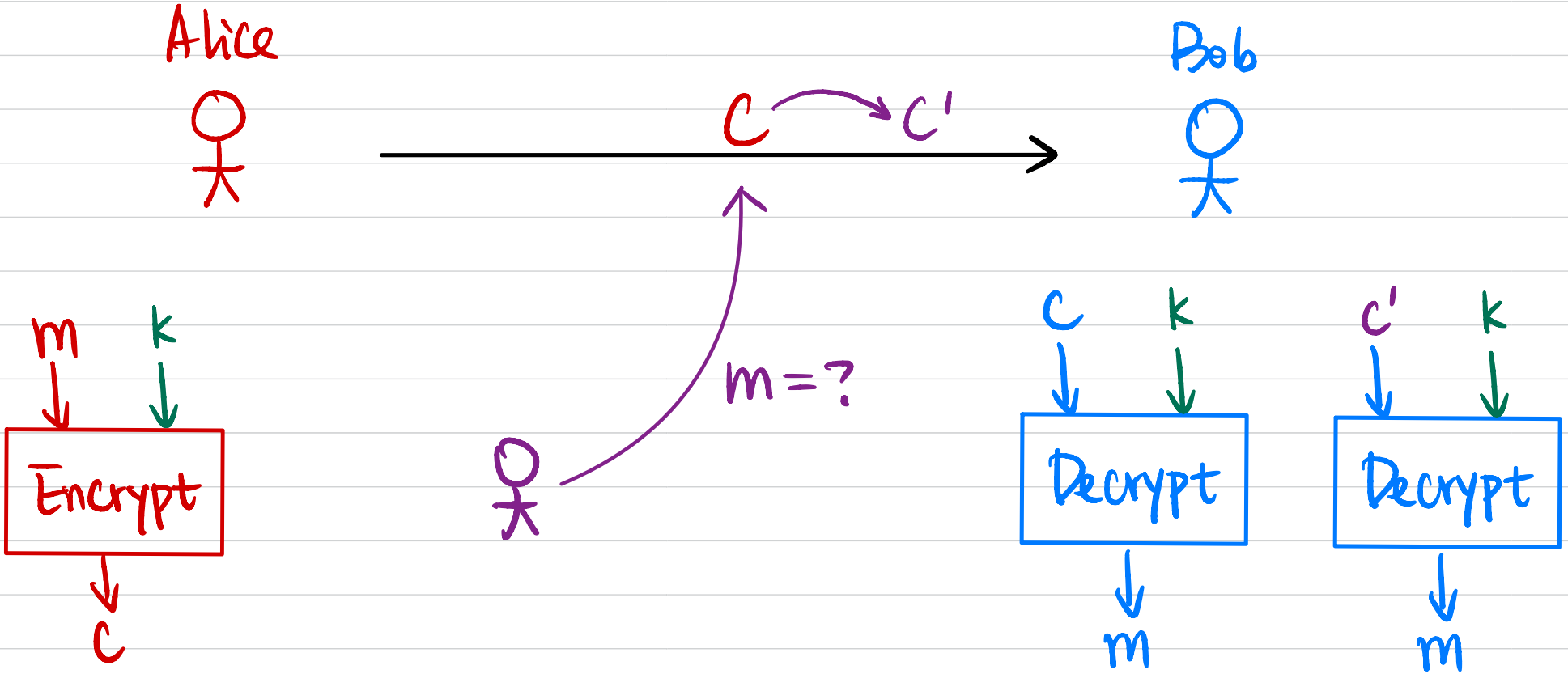
CSCI 1510

This Lecture:

- CCA-Security & Unforgeability
- Authenticated Encryption
- Generic Constructions

Authenticated Encryption

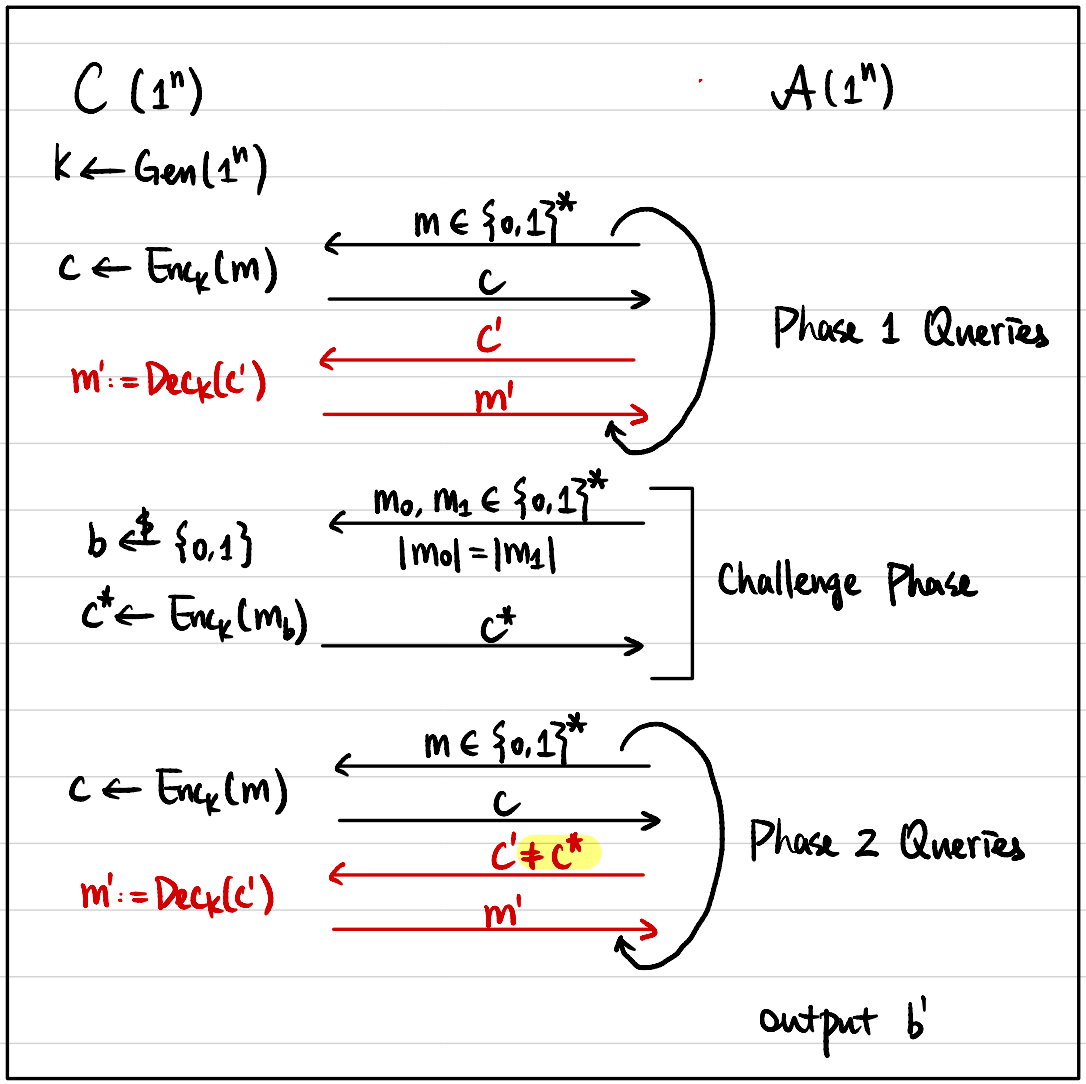


Security Guarantees:

- Message Secrecy: CCA Security
- Message Integrity: Unforgeability

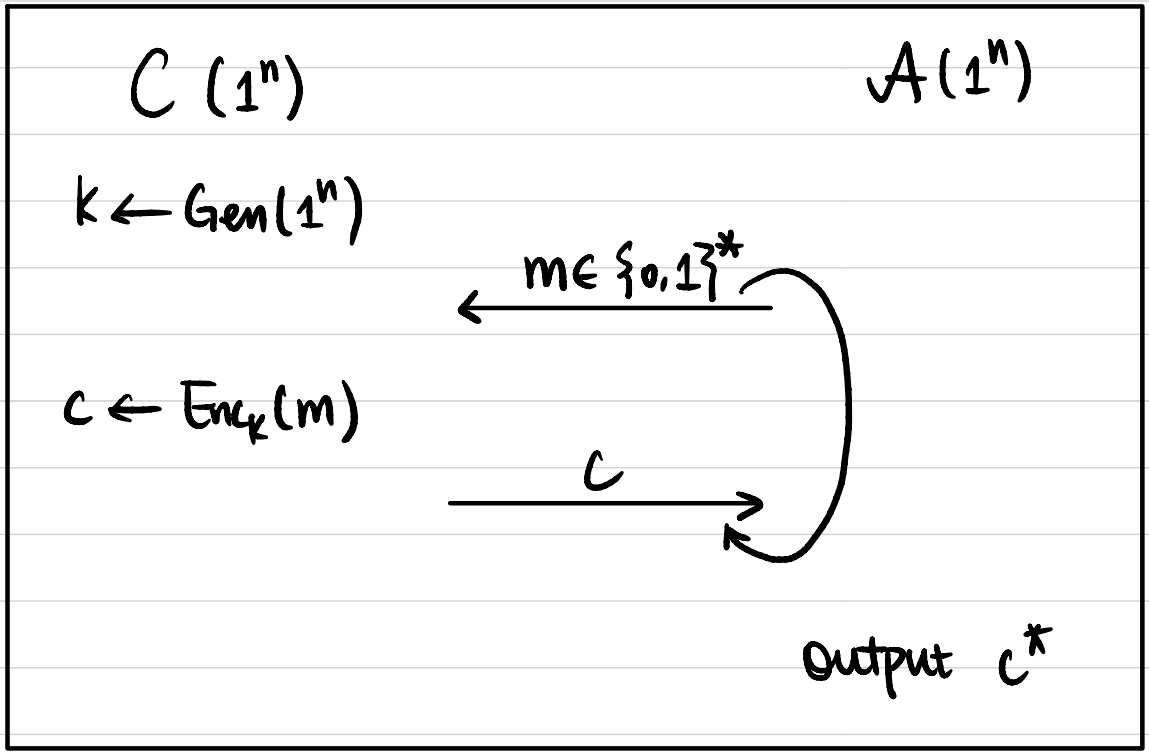
Chosen Ciphertext Attack (CCA) Security

Def A symmetric-key encryption scheme (Gen, Enc, Dec) is **secure against chosen ciphertext attacks**, or **CCA-secure**, if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$



Unforgeability

Def A symmetric-key encryption scheme $\Pi = (Gen, Enc, Dec)$ is **unforgeable** if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[EncForge_{\mathcal{A},\Pi} = 1] \leq \varepsilon(n)$.



$Q := \{m \mid m \text{ queried by } \mathcal{A}\}$

$m^* := Dec_k(c^*)$

$EncForge_{\mathcal{A},\Pi} = 1$ ($\mathcal{A}$ succeeds) if

① $m^* \notin Q$, and

② $m^* \neq \perp$

Def A symmetric-key encryption scheme is **authenticated encryption** if it is **CCA-secure** and **unforgeable**.

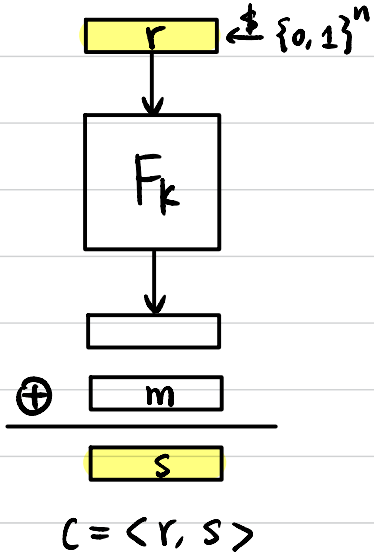
Exercises

Is the CPA-secure encryption from PRF CCA-secure? Unforgeable?

$\text{Enc}_k(m)$: $m \in \{0,1\}^n$

$r \xleftarrow{\$} \{0,1\}^n$

output $C := \langle r, F_k(r) \oplus m \rangle$



Generic Constructions

Let $\Pi^E = (Gen^E, Enc^E, Dec^E)$ be a CPA-secure encryption scheme.

Let $\Pi^M = (Gen^M, Mac^M, Vrfy^M)$ be a strongly secure MAC scheme.

How to construct an authenticated encryption scheme?

① Encrypt-and-Authenticate

② Authenticate-then-Encrypt

③ Encrypt-then-Authenticate

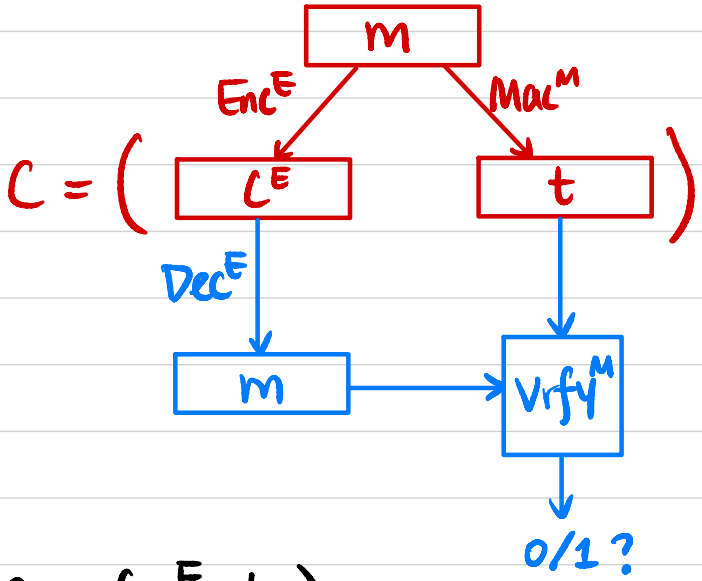
Encrypt-and-Authenticate

$\mathrm{Gen}(1^n)$:

$k^E \leftarrow \mathrm{Gen}^E(1^n)$

$k^M \leftarrow \mathrm{Gen}^M(1^n)$

Output $k = (k^E, k^M)$



$\mathrm{Enc}_k(m)$:

$C^E \leftarrow \mathrm{Enc}^E(k^E, m)$

$t \leftarrow \mathrm{Mac}^M(k^M, m)$

Output $C = (C^E, t)$

$\mathrm{Dec}_k(c)$: $C = (C^E, t_2)$

$m := \mathrm{Dec}^E(k^E, C^E)$

$b := \mathrm{Vrfy}^M(k^M, (m, t))$

If $b=1$, output m

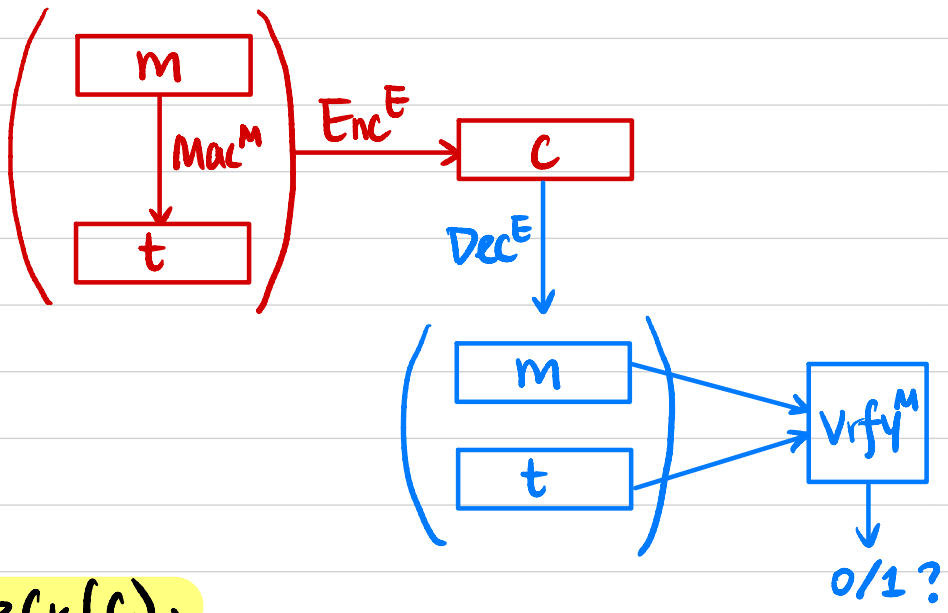
Otherwise output $\perp$

Q_1: Is it CPA-secure?

Q_2: Is it CCA-secure?

Q_3: Is it unforgeable?

Authenticate-then-Encrypt



$Gen(1^n)$:

$k^E \leftarrow Gen^E(1^n)$

$k^M \leftarrow Gen^M(1^n)$

Output $k = (k^E, k^M)$

$Enc_k(m)$:

$t \leftarrow Mac^M(k^M, m)$

$c \leftarrow Enc^E(k^E, m||t)$

output c

$Dec_k(c)$:

$m||t := Dec^E(k^E, c)$

$b := Vrfy^M(k^M, (m, t))$

If $b=1$, output m

Otherwise output $\perp$

Q_1: Is it CPA-secure? (exercise)

Q_2: Is it CCA-secure?

Q_3: Is it unforgeable? (exercise)

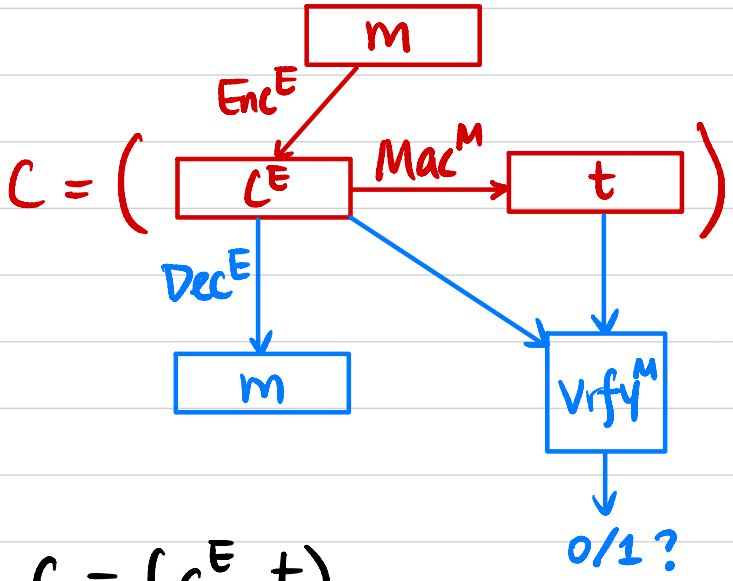
Encrypt-then-Authenticate

$\mathrm{Gen}(1^n)$:

$k^E \leftarrow \mathrm{Gen}^E(1^n)$

$k^M \leftarrow \mathrm{Gen}^M(1^n)$

Output $k = (k^E, k^M)$



$\mathrm{Enc}_k(m)$:

$c^E \leftarrow \mathrm{Enc}^E(k^E, m)$

$t \leftarrow \mathrm{Mac}^M(k^M, c^E)$

Output $c = (c^E, t)$

$\mathrm{Dec}_k(c)$: $c = (c^E, t)$

$m := \mathrm{Dec}^E(k^E, c^E)$

$b := \mathrm{Vrfy}^M(k^M, (c^E, t))$

If $b=1$, output m

Otherwise output $\perp$

Q_1: Is it CPA-secure? (exercise)

Q_2: Is it CCA-secure?

Q_3: Is it unforgeable? (exercise)

Intuitions

Can we have an encryption scheme that is unforgeable but not CCA-secure?

Can we have an encryption scheme that is CCA-secure but not unforgeable?