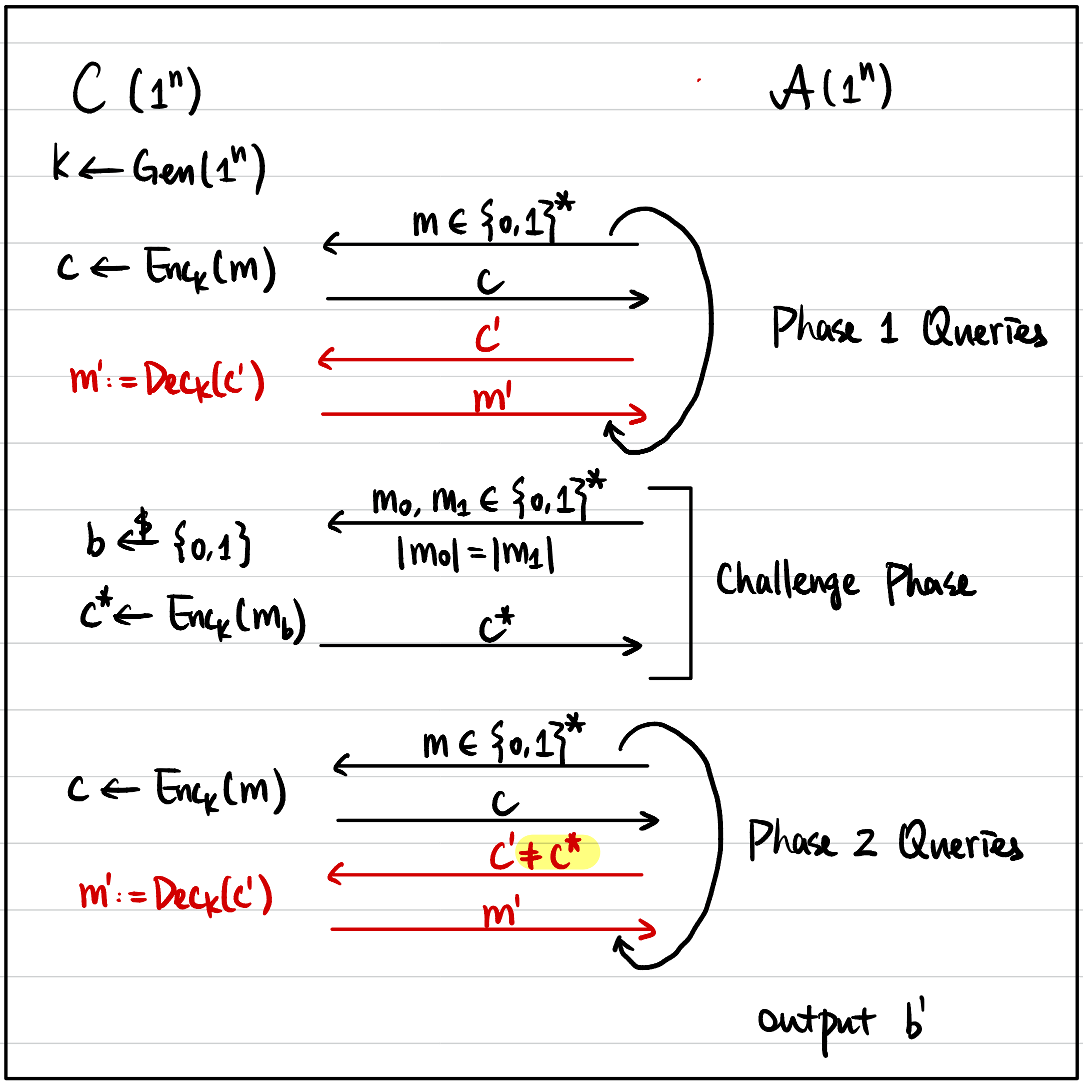
CSCI 1510

- Generic Constructions of Authenticated Encryption
- Collision-Resistant Hash Function

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 $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b=b'] \le \frac{1}{2} + \varepsilon(n)$



Unforgeability

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

$C(1^n)$ $\qquad\qquad\qquad\qquad$ $\mathcal{A}(1^n)$

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

$\xleftarrow{\quad m \in \{0,1\}^* \quad}$

$c \leftarrow \mathrm{Enc}_k(m)$

$\xrightarrow{\quad c \quad}$

output c^*

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

$m^* := \mathrm{Dec}_k(c^*)$

$\mathrm{EncForge}_{\mathcal{A},\Pi} = 1$ ($\mathcal{A}$ 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.

Intuitions

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

$ct \to ct'$ encrypting the same message

But hard to generate a new ct encrypting a new message

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

Generic Constructions

Let $\Pi^E = (\mathrm{Gen}^E, \mathrm{Enc}^E, \mathrm{Dec}^E)$ be a CPA-secure encryption scheme.
Let $\Pi^M = (\mathrm{Gen}^M, \mathrm{Mac}^M, \mathrm{Vrfy}^M)$ be a strongly secure MAC scheme.

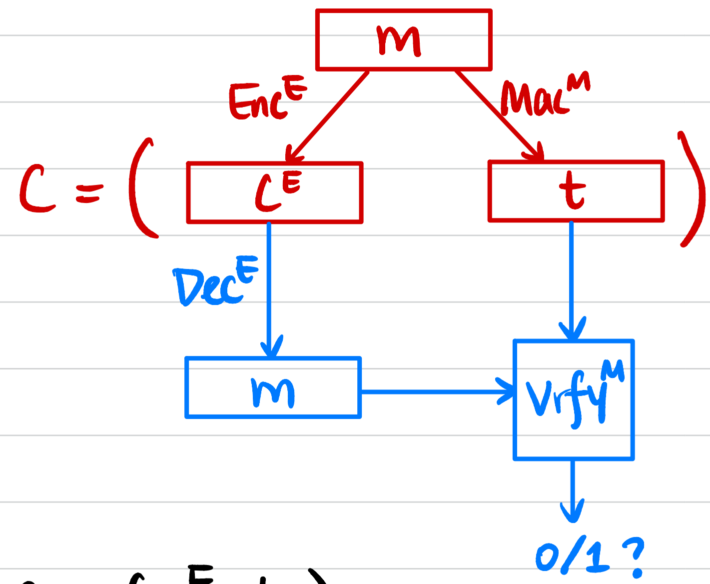
How to construct an authenticated encryption scheme?

① Encrypt-and-Authenticate

② Authenticate-then-Encrypt

③ Encrypt-then-Authenticate

Encrypt-and-Authenticate



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):

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

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

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

Dec$_k$(c): $c = (c^E, t_2)$

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

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

If $b = 1$, output m

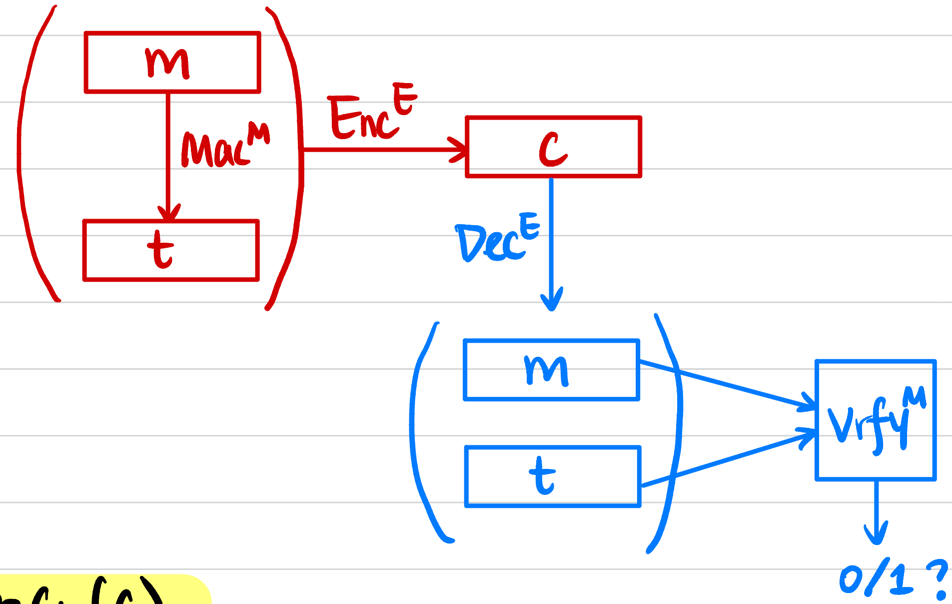
Otherwise output $\perp$

Q1: Is it CPA-secure?

Q2: Is it CCA-secure?

Q3: 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

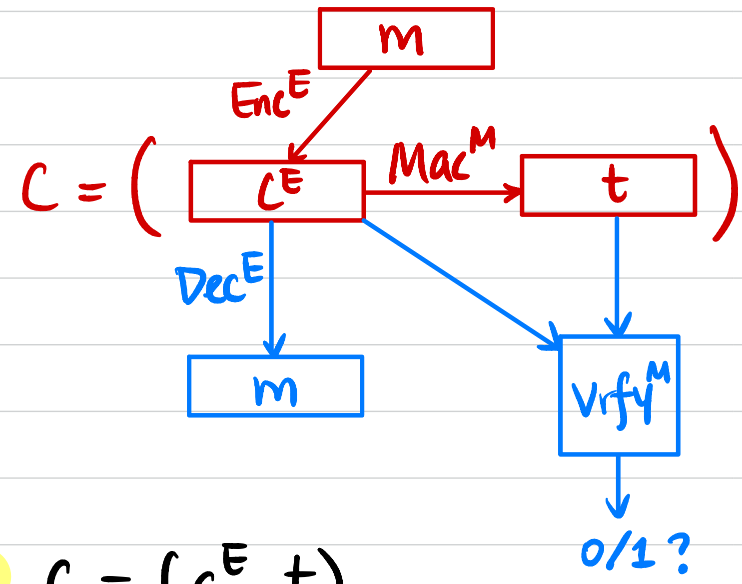
Otherwise output $\perp$

Q1: Is it CPA-secure? (exercise)

Q2: Is it CCA-secure?

Q3: Is it unforgeable? (exercise)

Encrypt-then-Authenticate



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):

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

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

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

Dec$_k$(c): $c = (c^E, t)$

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

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

If $b = 1$, output m

Otherwise output $\perp$

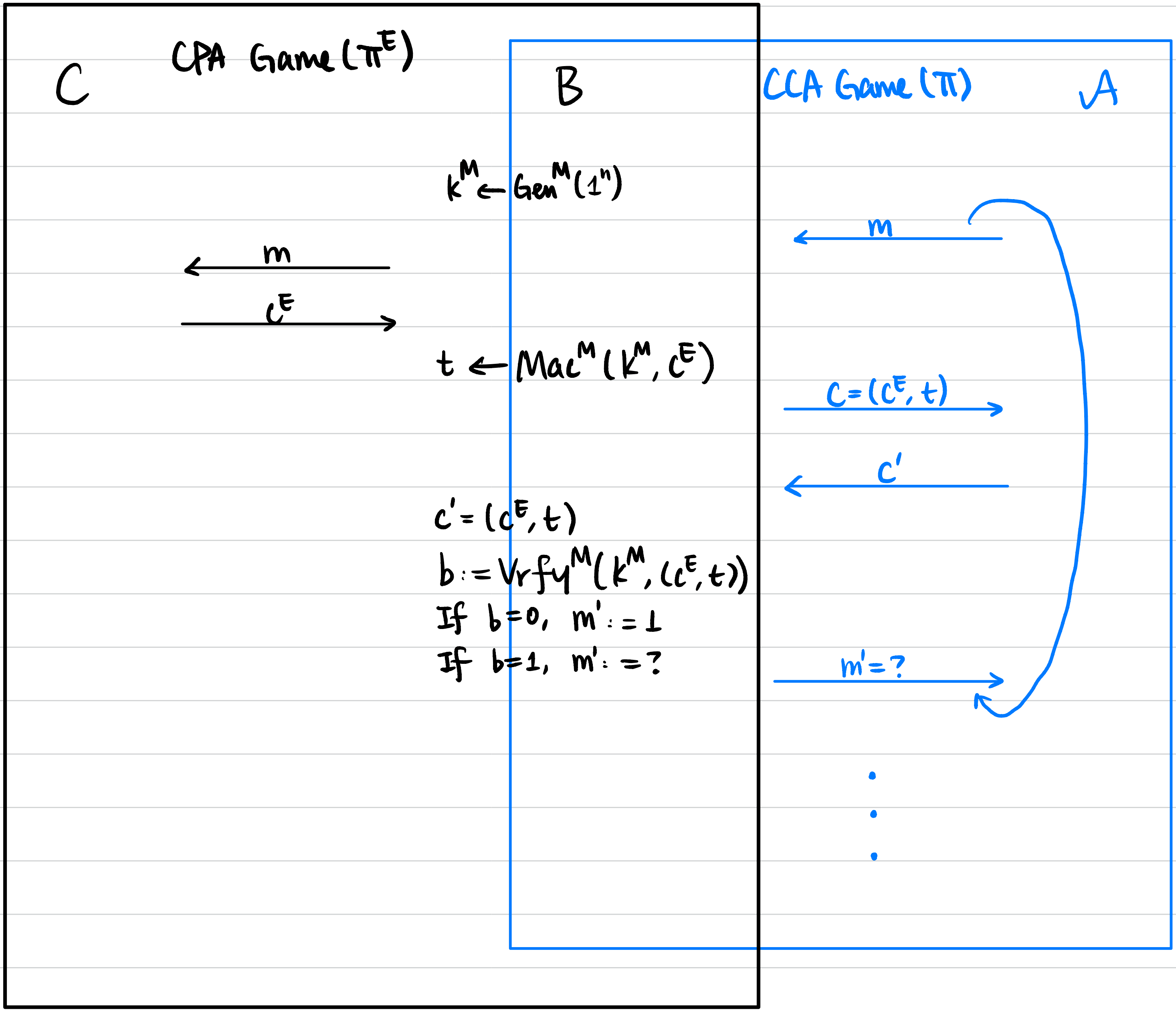
Q1: Is it CPA-secure ?

Q2: Is it CCA-secure ?

Q3: Is it unforgeable ? (exercise)

First Attempt: Assume $\exists$ PPT $\mathcal{A}$ that breaks the CCA-security of Π

We construct PPT $\mathcal{B}$ to break the CPA-security of Π^E.

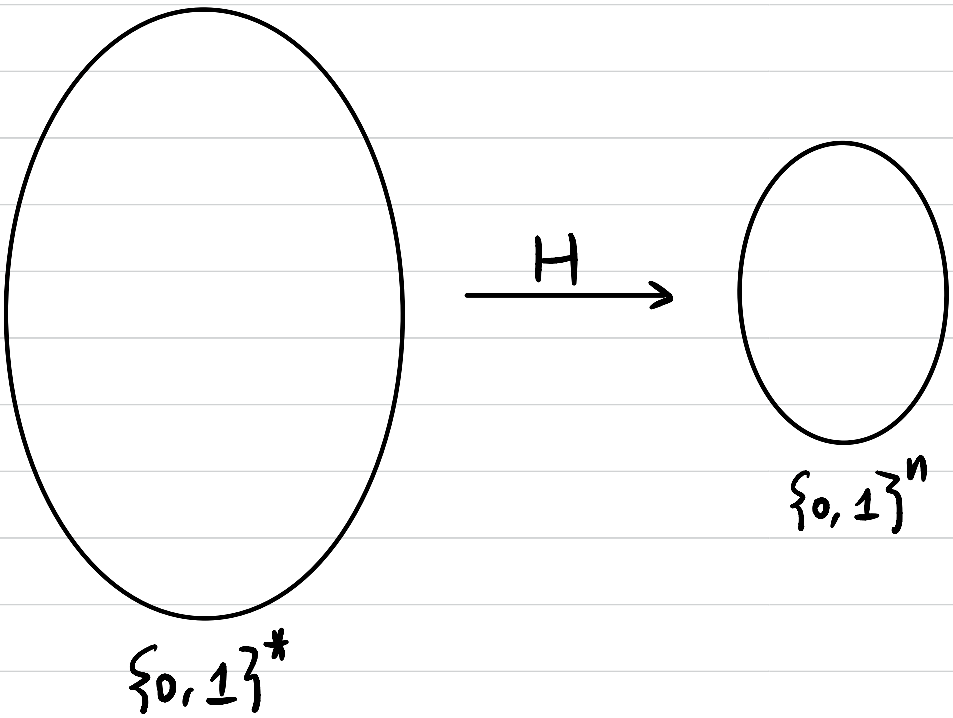


$\mathcal{C}(1^n)$	$\mathcal{H}_0$	$\mathcal{A}(1^n)$
$k^E \leftarrow Gen^E(1^n)$		
$k^M \leftarrow Gen^M(1^n)$		
	$\xleftarrow{\quad m \quad}$	
$c^E \leftarrow Enc^E(k^E, m)$		
$t \leftarrow Mac^M(k^M, c^E)$	$\xrightarrow{c=(c^E, t)}$	
	$\xleftarrow{\quad c \quad}$	
$c=(c^E, t)$		
$\tilde{b} := Vrfy^M(k^M, (c^E, t))$		
If $\tilde{b}=1$, $m := Dec^E(k^E, c^E)$		
Otherwise $m := \perp$	$\xrightarrow{\quad m \quad}$	
	$\xleftarrow{m_0,\ m_1}$	
$b \xleftarrow{\$} \{0,1\}$		
$c^{E*} \leftarrow Enc^E(k^E, m_b)$		
$t^* \leftarrow Mac^M(k^M, c^{E*})$	$\xrightarrow{c^*=(c^{E*}, t^*)}$	
	$\xleftarrow{\quad m \quad}$	
	$\xrightarrow{c=(c^E, t)}$	
	$\xleftarrow{c \neq c^*}$	
	$\xrightarrow{\quad m \quad}$	Output b'

$\mathcal{C}(1^n)$	$\mathcal{H}_1$	$\mathcal{A}(1^n)$
$k^E \leftarrow Gen^E(1^n)$		
$k^M \leftarrow Gen^M(1^n)$		
	$\xleftarrow{\quad m \quad}$	
$c^E \leftarrow Enc^E(k^E, m)$		
$t \leftarrow Mac^M(k^M, c^E)$	$\xrightarrow{c=(c^E, t)}$	
	$\xleftarrow{\quad c \quad}$	
$c=(c^E, t)$		
If c is encryption of m queried by $\mathcal{A}$, reply m;		
Otherwise reply $\perp$	$\xrightarrow{\quad m \quad}$	
	$\xleftarrow{m_0,\ m_1}$	
$b \xleftarrow{\$} \{0,1\}$		
$c^{E*} \leftarrow Enc^E(k^E, m_b)$		
$t^* \leftarrow Mac^M(k^M, c^{E*})$	$\xrightarrow{c^*=(c^{E*}, t^*)}$	
	$\xleftarrow{\quad m \quad}$	
	$\xrightarrow{c=(c^E, t)}$	
	$\xleftarrow{c \neq c^*}$	
	$\xrightarrow{\quad m \quad}$	Output b'

Cryptographic Hash Function

$$H: \{0,1\}^* \longrightarrow \{0,1\}^n$$



Collision-Resistant Hash Function (CRHF):

It's computationally hard to find $x, x' \in \{0,1\}^*$ s.t.

$x \neq x'$, $H(x) = H(x')$ (collision)

Collision-Resistant Hash Function (CRHF)

- **Syntax:**

  A hash function is defined by a pair of PPT algorithms (Gen, H):
  - $\mathrm{Gen}(1^n)$: output s
  - $H^s(x)$: $x \in \{0,1\}^*$, output $h \in \{0,1\}^{\ell(n)}$

- **Security**

  A hash function (Gen, H) is collision-resistant if

  $\forall$PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[x \neq x' \wedge H^s(x) = H^s(x')] \le \varepsilon(n)$.

$C(1^n)$		$\mathcal{A}(1^n)$
$s \leftarrow \mathrm{Gen}(1^n)$	$\xrightarrow{\quad s \quad}$	
		output (x, x')

How to find a collision?

$$H^s : \{0,1\}^* \longrightarrow \{0,1\}^\ell$$

Try $H^s(x_1), H^s(x_2), \cdots, H^s(x_q)$

If $H(x_i)$ outputs a random value,

what's the probability of finding a collision?

If $q = 2^\ell + 1 \Rightarrow$ prob. $= 1$

If $q = 2 \Rightarrow$ prob. $= ?$

If $q = k \Rightarrow$ prob. $= ?$

Birthday Problem / Paradox

There are q students in a class.

Assume each student's birthday is a random $y_i \xleftarrow{\$} [365]$

What's the probability of a collision?

$q = 366 \Rightarrow$ prob. $= 1$

$q = 23 \Rightarrow$ prob. $\simeq 50\%$

$q = 70 \Rightarrow$ prob. $\simeq 99.9\%$

$y_i \xleftarrow{\$} [N]$

$q = N+1 \Rightarrow$ prob. $= 1$

$q = \sqrt{N} \Rightarrow$ prob. $\simeq 50\%$

If security parameter $n = 128$, $\ell = ?$