# II – Encryption

David Pointcheval

MPRI – Paris

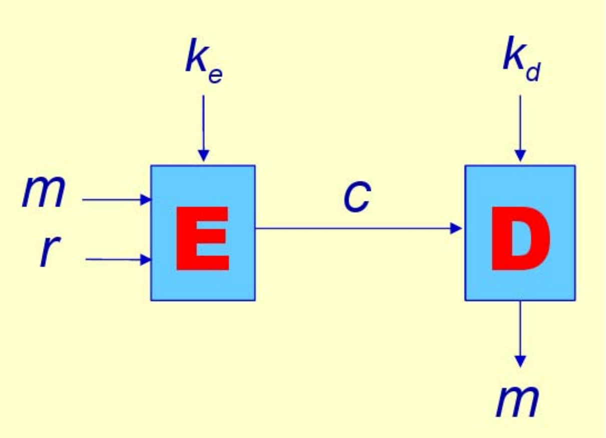
Ecole normale supérieure/PSL, CNRS & INRIA

# Outline

# Basic Security Notions

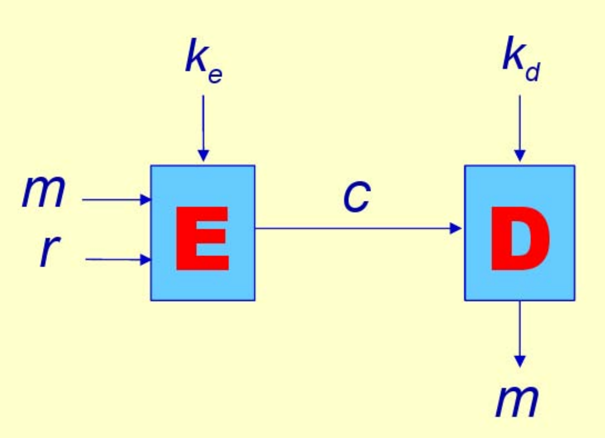
# Outline

# Public-Key Encryption



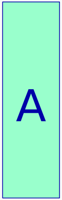

Goal: Privacy/Secrecy of the plaintext

# Public-Key Encryption

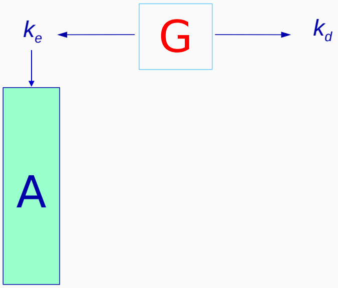



Goal: Privacy/Secrecy of the plaintext

# $\mathrm{OW}-\mathrm{CPA}$ Security Game



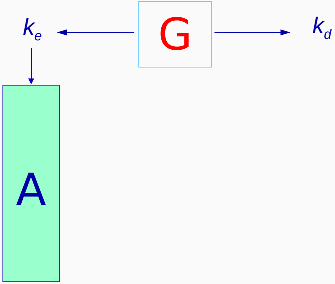
## OW − CPA Security Game



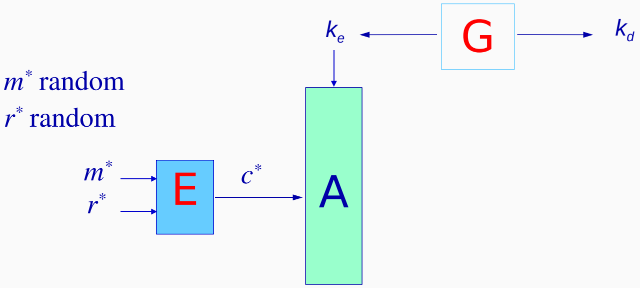
# OW − CPA Security Game

$m^*$ random

$r^*$ random



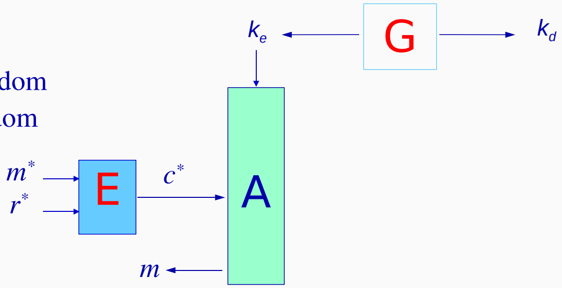
# OW − CPA Security Game



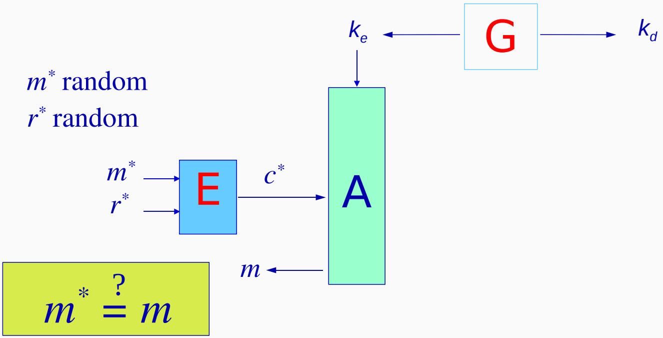
# $\mathrm{OW}-\mathrm{CPA}$ Security Game

$m^*$ random

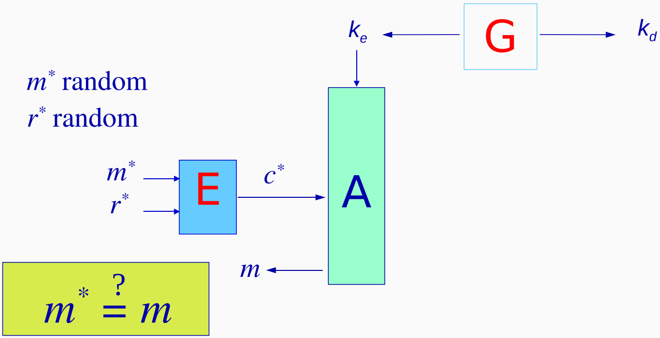
$r^*$ random



# OW − CPA Security Game

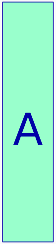


# OW − CPA Security Game

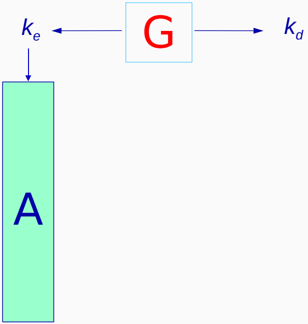



$$\mathbf{Succ}_{\mathcal{S}}^{\mathsf{ow}}(\mathcal{A}) = \Pr[(sk, pk) \leftarrow \mathcal{K}(); m \stackrel{R}{\leftarrow} \mathcal{M}; c = \mathcal{E}_{pk}(m) : \mathcal{A}(pk, c) \rightarrow m]$$

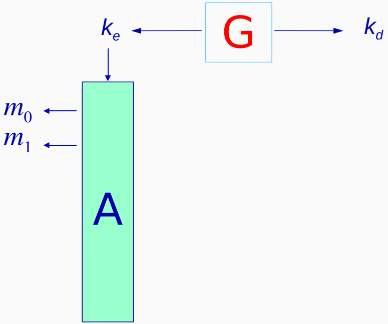
# IND − CPA Security Game



# $\mathsf{IND} - \mathsf{CPA}$ Security Game



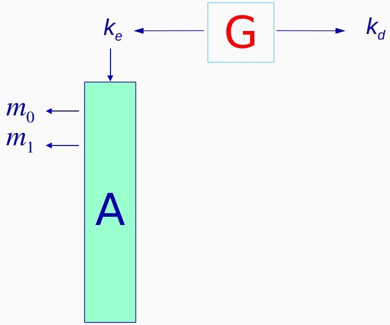
# $\mathrm{IND} - \mathrm{CPA}$ Security Game



# IND − CPA Security Game

$b \in \{0,1\}$

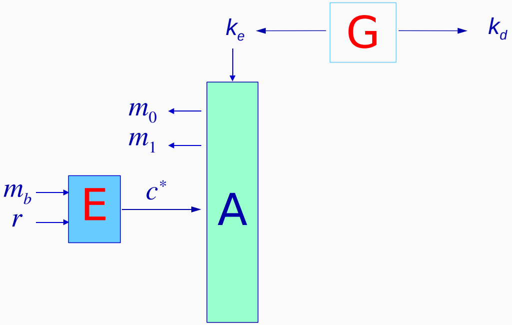
$r$ random



# IND − CPA Security Game

$b \in \{0,1\}$

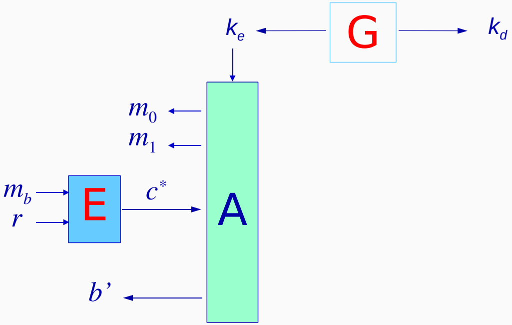
$r$ random



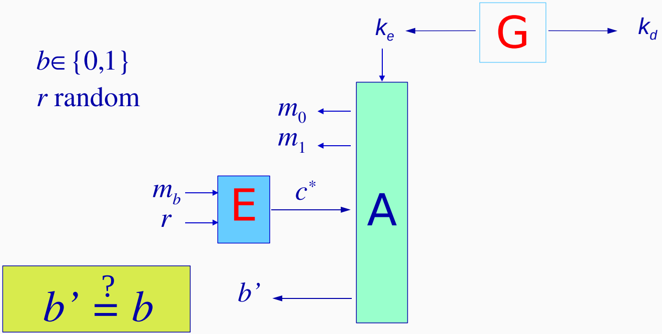
# $\mathrm{IND}-\mathrm{CPA}$ Security Game

$b \in \{0,1\}$

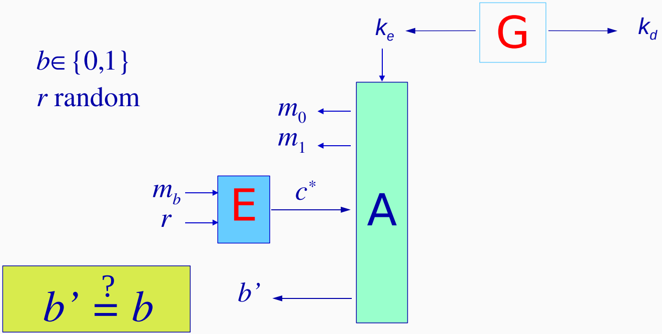
$r$ random



# IND – CPA Security Game



# $\mathbf{IND-CPA}$ Security Game




$$(sk, pk) \leftarrow \mathcal{K}(); (m_0, m_1, \text{state}) \leftarrow \mathcal{A}(pk);$$

$$b \stackrel{R}{\leftarrow} \{0,1\}; c = \mathcal{E}_{pk}(m_b); b' \leftarrow \mathcal{A}(\text{state}, c)$$

$$\mathbf{Adv}_{\mathcal{S}}^{\text{ind}-\text{cpa}}(\mathcal{A}) = \left|\Pr[b' = 1 | b = 1] - \Pr[b' = 1 | b = 0]\right| = \left|2 \times \Pr[b' = b] - 1\right|$$

# Outline

**Basic Security Notions**

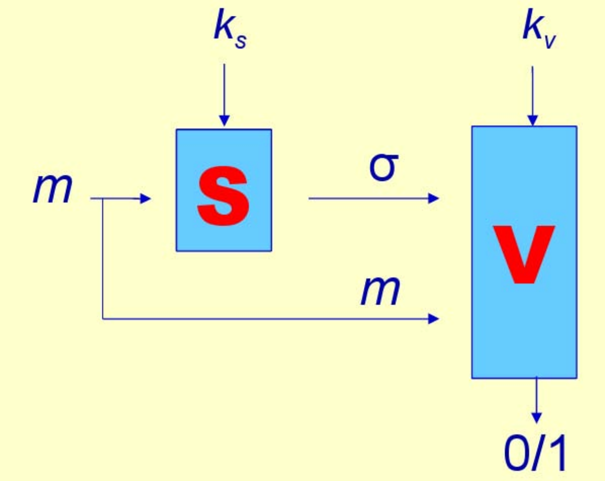
- Public-Key Encryption
- Signatures

**Game-based Proofs**

**Advanced Security for Encryption**

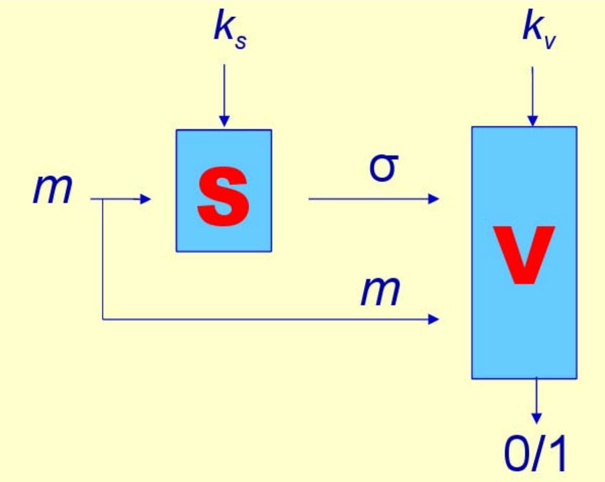
**Conclusion**

# Signature



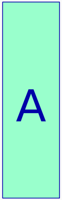

Goal: Authentication of the sender

# Signature

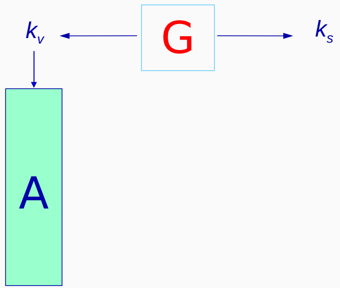



Goal: Authentication of the sender

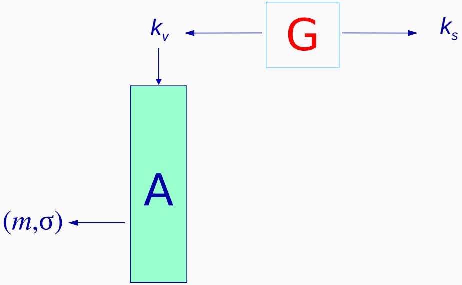
# EUF − NMA



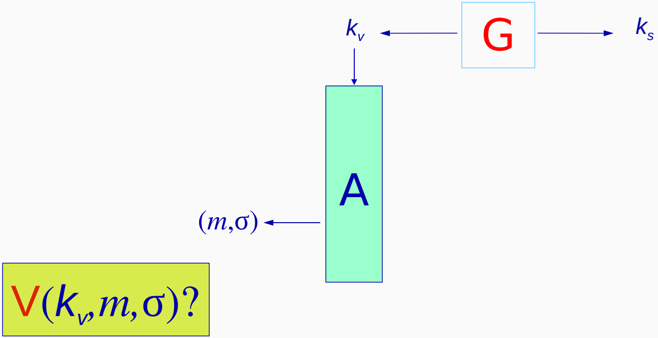
# $\mathsf{EUF} - \mathsf{NMA}$



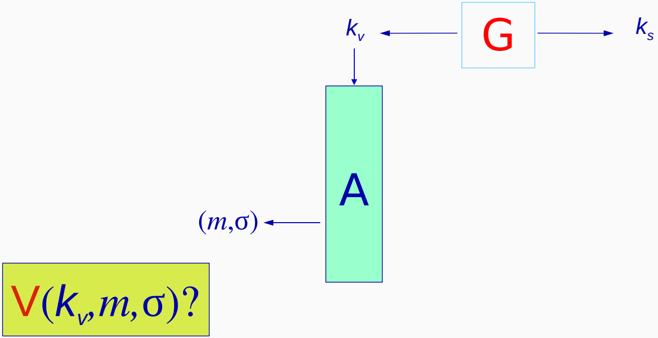
# EUF – NMA



# EUF – NMA



# EUF − NMA




$$\mathbf{Succ}^{\mathsf{euf}}_{\mathcal{SG}}(\mathcal{A}) = \Pr[(sk, pk) \leftarrow \mathcal{K}(); (m, \sigma) \leftarrow \mathcal{A}(pk) : \mathcal{V}_{pk}(m, \sigma) = 1]$$

# Game-based Proofs

# Outline

## Provable Security

One can prove that:

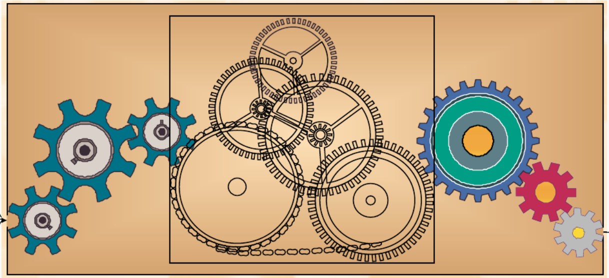
- if an adversary is able to break the cryptographic scheme
- then one can break the underlying problem
  (integer factoring, discrete logarithm, 3-SAT, etc)

# Provable Security

One can prove that:

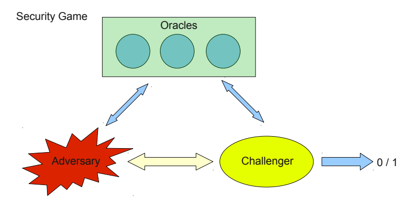
- if an adversary is able to break the cryptographic scheme
- then one can break the underlying problem
  (integer factoring, discrete logarithm, 3-SAT, etc)

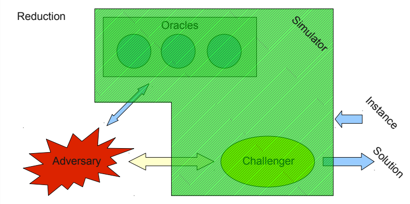
hard instance $\rightarrow$



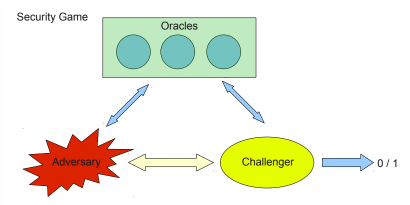
$\rightarrow$ solution

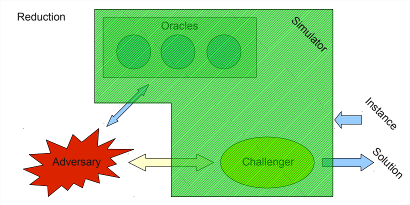
# Direct Reduction



# Direct Reduction

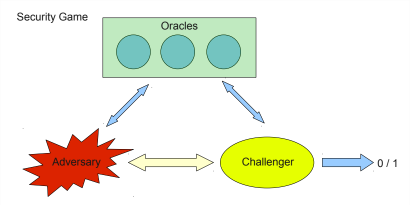


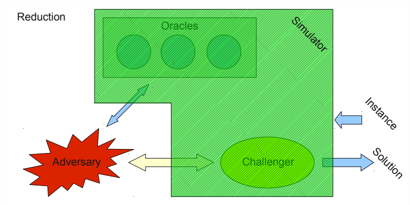




Unfortunately

- Security may rely on several assumptions
- Proving that the view of the adversary, generated by the simulator, in the reduction is the same as in the real attack game is not easy to do in such a one big step

# Direct Reduction

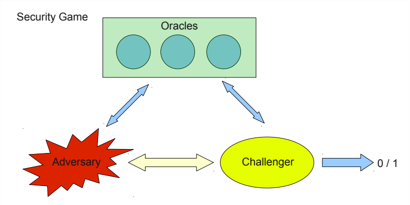


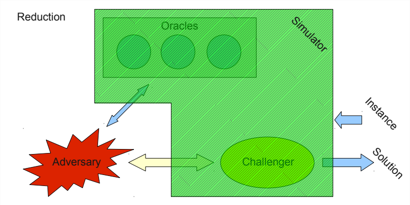




Unfortunately

- Security may rely on several assumptions
- Proving that the view of the adversary, generated by the simulator, in the reduction is the same as in the real attack game is not easy to do in such a one big step

# Direct Reduction




Unfortunately

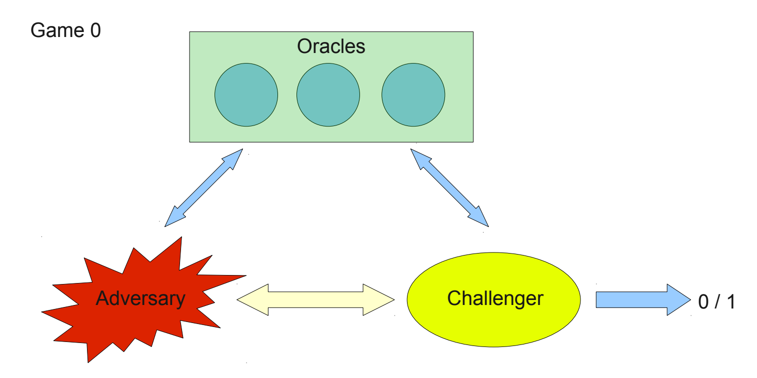
- Security may rely on several assumptions
- Proving that the view of the adversary, generated by the simulator, in the reduction is the same as in the real attack game is not easy to do in such a one big step

# Outline

# Sequence of Games

## Real Attack Game

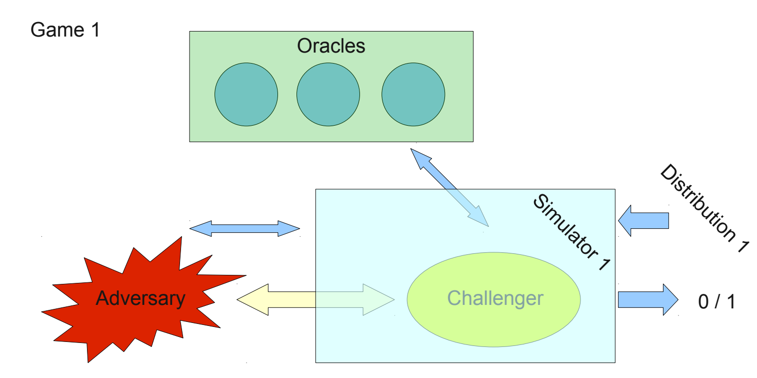
The adversary plays a game, against a challenger (security notion)



# Sequence of Games

## Simulation

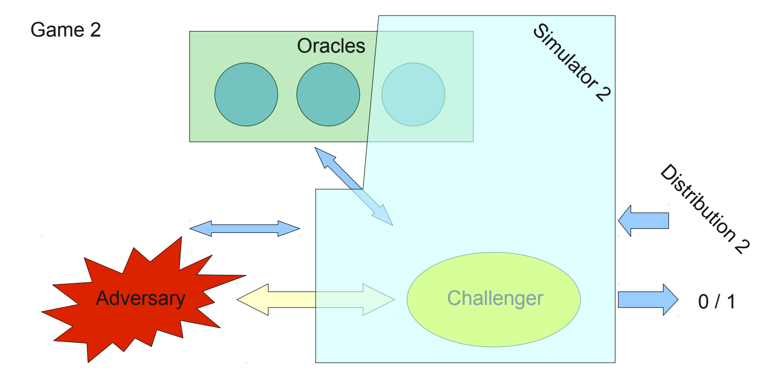
The adversary plays a game, against a sequence of simulators



# Sequence of Games

## Simulation

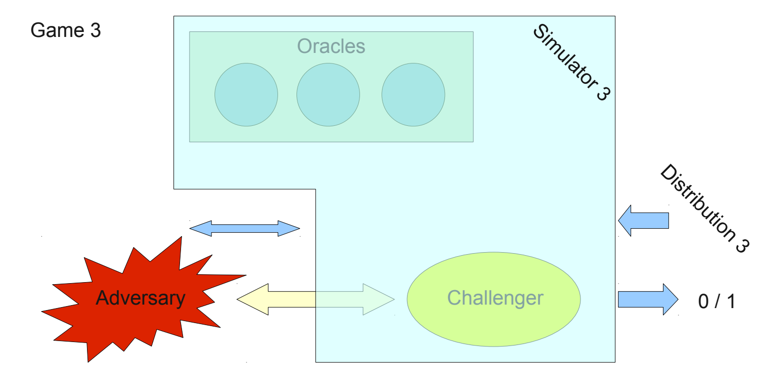
The adversary plays a game, against a sequence of simulators



# Sequence of Games

## Simulation

The adversary plays a game, against a sequence of simulators



# Output

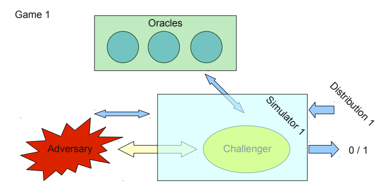
- The output of the simulator in Game 1 is related to the output of the challenger in Game 0 (adversary's winning probability)
- The output of the simulator in Game 3 is easy to evaluate (e.g. always zero, always 1, probability of one-half)
- The gaps (Game 1 $\leftrightarrow$ Game 2, Game 2 $\leftrightarrow$ Game 3, etc) are clearly identified with specific events

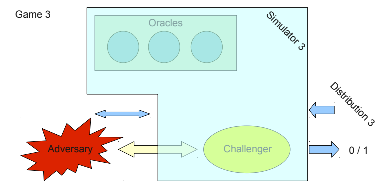
# Output

- The output of the simulator in Game 1 is related to the output of the challenger in Game 0 (adversary's winning probability)
- The output of the simulator in Game 3 is easy to evaluate (e.g. always zero, always 1, probability of one-half)
- The gaps (Game 1 $\leftrightarrow$ Game 2, Game 2 $\leftrightarrow$ Game 3, etc) are clearly identified with specific events

# Output

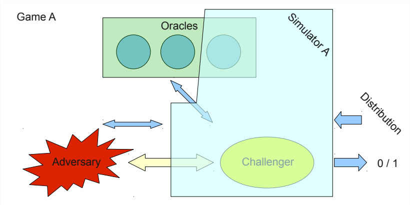
- The output of the simulator in Game 1 is related to the output of the challenger in Game 0 (adversary's winning probability)
- The output of the simulator in Game 3 is easy to evaluate (e.g. always zero, always 1, probability of one-half)
- The gaps (Game 1 $\leftrightarrow$ Game 2, Game 2 $\leftrightarrow$ Game 3, etc) are clearly identified with specific events

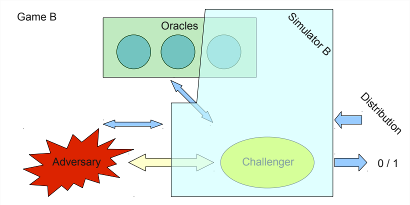


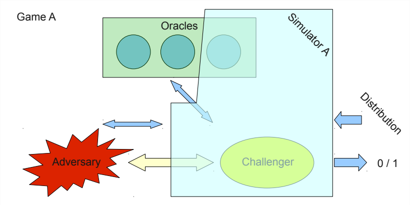
# Outline

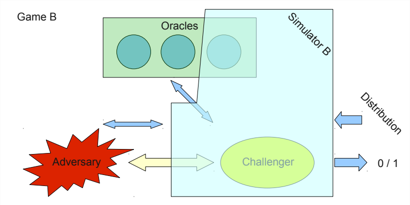
# Two Simulators



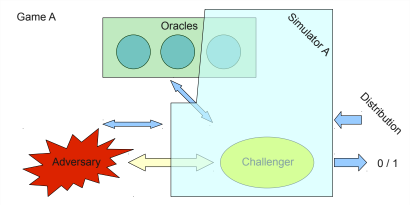
# Two Simulators

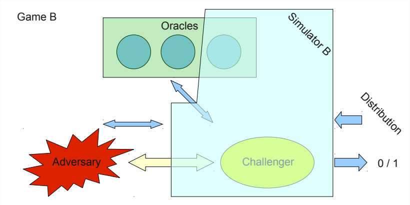



- perfectly identical behaviors **[Hop-S-Perfect]**
- different behaviors, only if event **Ev** happens
  - **Ev** is negligible **[Hop-S-Negl]**
  - **Ev** is non-negligible (but not overwhelming) **[Hop-S-Non-Negl]**
    and independent of the output in Game$_A$
    $\rightarrow$ Simulator B terminates in case of event Ev

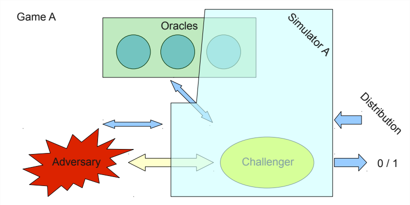
# Two Simulators

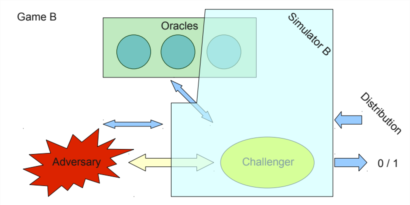



- perfectly identical behaviors [Hop-S-Perfect]
- different behaviors, only if event **Ev** happens
  - **Ev** is negligible [Hop-S-Negl]
  - **Ev** is non-negligible (but not overwhelming) and independent of the output in $\textbf{Game}_A$ [Hop-S-Non-Negl]
    $\rightarrow$ Simulator B terminates in case of event **Ev**

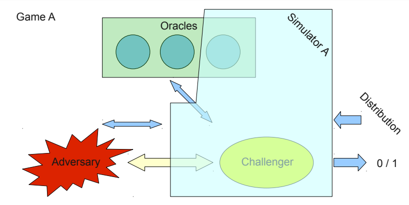
# Two Simulators

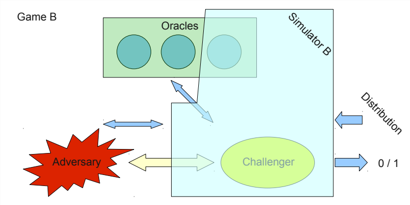



- perfectly identical behaviors [**Hop-S-Perfect**]
- different behaviors, only if event **Ev** happens
  - **Ev** is negligible [**Hop-S-Negl**]
  - **Ev** is non-negligible (but not overwhelming) and independent of the output in **Game**$_A$ [**Hop-S-Non-Negl**]
    $\rightarrow$ Simulator B terminates in case of event **Ev**

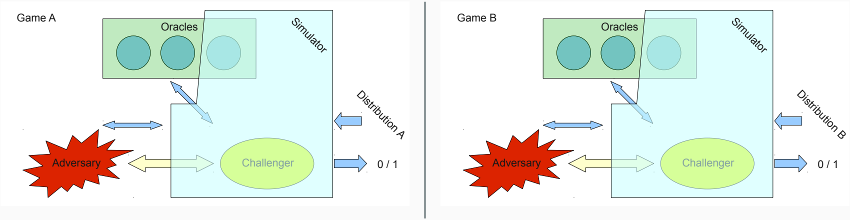
# Two Simulators



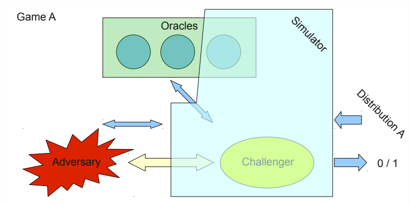



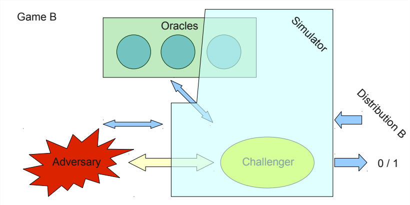

- perfectly identical behaviors **[Hop-S-Perfect]**
- different behaviors, only if event **Ev** happens
  - **Ev** is negligible **[Hop-S-Negl]**
  - **Ev** is non-negligible (but not overwhelming) **[Hop-S-Non-Negl]** and independent of the output in $\mathbf{Game}_A$
    $\rightarrow$ Simulator B terminates in case of event **Ev**

# Two Distributions



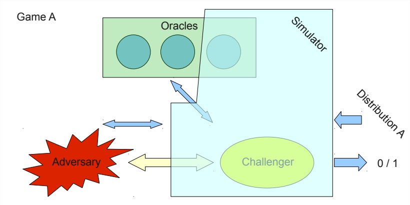
# Two Distributions

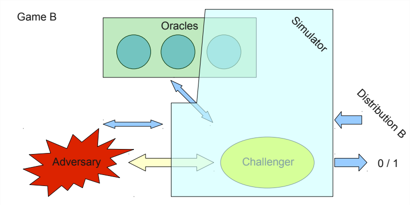



- perfectly identical input distributions **[Hop-D-Perfect]**
- different distributions
  - statistically close **[Hop-D-Stat]**
  - computationally close **[Hop-D-Comp]**

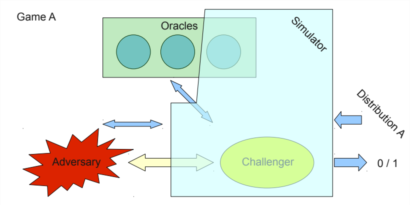
# Two Distributions

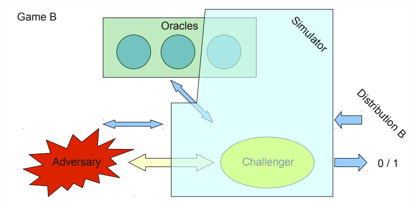



- perfectly identical input distributions [Hop-D-Perfect]
- different distributions
  - statistically close [Hop-D-Stat]
  - computationally close [Hop-D-Comp]

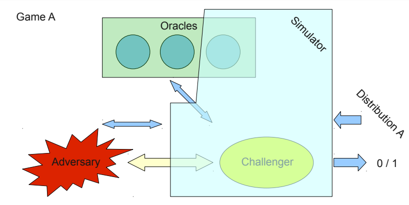
# Two Distributions

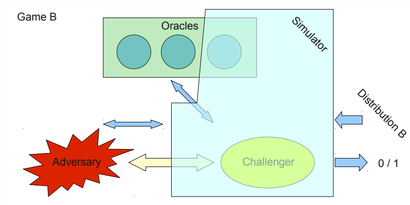



- perfectly identical input distributions **[Hop-D-Perfect]**
- different distributions
  - statistically close **[Hop-D-Stat]**
  - computationally close **[Hop-D-Comp]**

# Two Distributions




- perfectly identical input distributions **[Hop-D-Perfect]**
- different distributions
  - statistically close **[Hop-D-Stat]**
  - computationally close **[Hop-D-Comp]**

# Two Simulations

- Identical behaviors: $\Pr[\mathbf{Game}_A] - \Pr[\mathbf{Game}_B] = 0$
- The behaviors differ only if **Ev** happens:
  - **Ev** is negligible, one can ignore it
    Shoup's Lemma: $|\Pr[\mathbf{Game}_A] - \Pr[\mathbf{Game}_B]| \leq \Pr[\mathbf{Ev}]$

$$
\begin{aligned}
&|\Pr[\mathbf{Game}_A] - \Pr[\mathbf{Game}_B]| \\
&= \left| \begin{array}{l} \Pr[\mathbf{Game}_A|\mathbf{Ev}]\Pr[\mathbf{Ev}] + \Pr[\mathbf{Game}_A|\neg\mathbf{Ev}]\Pr[\neg\mathbf{Ev}] \\ -\Pr[\mathbf{Game}_B|\mathbf{Ev}]\Pr[\mathbf{Ev}] - \Pr[\mathbf{Game}_B|\neg\mathbf{Ev}]\Pr[\neg\mathbf{Ev}] \end{array} \right| \\
&= \left| \begin{array}{l} (\Pr[\mathbf{Game}_A|\mathbf{Ev}] - \Pr[\mathbf{Game}_B|\mathbf{Ev}]) \times \Pr[\mathbf{Ev}] \\ +(\Pr[\mathbf{Game}_A|\neg\mathbf{Ev}] - \Pr[\mathbf{Game}_B|\neg\mathbf{Ev}]) \times \Pr[\neg\mathbf{Ev}] \end{array} \right| \\
&\leq |1 \times \Pr[\mathbf{Ev}] + 0 \times \Pr[\neg\mathbf{Ev}]| \leq \Pr[\mathbf{Ev}]
\end{aligned}
$$

  - **Ev** is non-negligible and independent of the output in $\mathbf{Game}_A$,
    Simulator B terminates in case of event **Ev**

# Two Simulations

- Identical behaviors: $\Pr[\mathbf{Game}_A] - \Pr[\mathbf{Game}_B] = 0$
- The behaviors differ only if **Ev** happens:
  - **Ev** is negligible, one can ignore it
    Shoup's Lemma: $|\Pr[\mathbf{Game}_A] - \Pr[\mathbf{Game}_B]| \leq \Pr[\mathbf{Ev}]$

$$
\begin{aligned}
&|\Pr[\mathbf{Game}_A] - \Pr[\mathbf{Game}_B]| \\
&= \left| \begin{array}{l} \Pr[\mathbf{Game}_A|\mathbf{Ev}]\Pr[\mathbf{Ev}] + \Pr[\mathbf{Game}_A|\neg\mathbf{Ev}]\Pr[\neg\mathbf{Ev}] \\ -\Pr[\mathbf{Game}_B|\mathbf{Ev}]\Pr[\mathbf{Ev}] - \Pr[\mathbf{Game}_B|\neg\mathbf{Ev}]\Pr[\neg\mathbf{Ev}] \end{array} \right| \\
&= \left| \begin{array}{l} (\Pr[\mathbf{Game}_A|\mathbf{Ev}] - \Pr[\mathbf{Game}_B|\mathbf{Ev}]) \times \Pr[\mathbf{Ev}] \\ +(\Pr[\mathbf{Game}_A|\neg\mathbf{Ev}] - \Pr[\mathbf{Game}_B|\neg\mathbf{Ev}]) \times \Pr[\neg\mathbf{Ev}] \end{array} \right| \\
&\leq |1 \times \Pr[\mathbf{Ev}] + 0 \times \Pr[\neg\mathbf{Ev}]| \leq \Pr[\mathbf{Ev}]
\end{aligned}
$$

  - **Ev** is non-negligible and independent of the output in $\mathbf{Game}_A$,
    Simulator B terminates in case of event **Ev**

# Two Simulations

- Identical behaviors: $\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] = 0$
- The behaviors differ only if **Ev** happens:
  - **Ev** is negligible, one can ignore it
    Shoup's Lemma: $|\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B]| \leq \Pr[\textbf{Ev}]$

$$
\begin{aligned}
& |\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B]| \\
= & \left| \begin{array}{l} \Pr[\textbf{Game}_A|\textbf{Ev}]\Pr[\textbf{Ev}] + \Pr[\textbf{Game}_A|\neg\textbf{Ev}]\Pr[\neg\textbf{Ev}] \\ - \Pr[\textbf{Game}_B|\textbf{Ev}]\Pr[\textbf{Ev}] - \Pr[\textbf{Game}_B|\neg\textbf{Ev}]\Pr[\neg\textbf{Ev}] \end{array} \right| \\
= & \left| \begin{array}{l} (\Pr[\textbf{Game}_A|\textbf{Ev}] - \Pr[\textbf{Game}_B|\textbf{Ev}]) \times \Pr[\textbf{Ev}] \\ +(\Pr[\textbf{Game}_A|\neg\textbf{Ev}] - \Pr[\textbf{Game}_B|\neg\textbf{Ev}]) \times \Pr[\neg\textbf{Ev}] \end{array} \right| \\
\leq & |1 \times \Pr[\textbf{Ev}] + 0 \times \Pr[\neg\textbf{Ev}]| \leq \Pr[\textbf{Ev}]
\end{aligned}
$$

  - **Ev** is non-negligible and independent of the output in $\textbf{Game}_A$,
    Simulator B terminates in case of event **Ev**

# Two Simulations

- Identical behaviors: $\Pr[\mathbf{Game}_A] - \Pr[\mathbf{Game}_B] = 0$
- The behaviors differ only if **Ev** happens:
  - **Ev** is negligible, one can ignore it
  - **Ev** is non-negligible and independent of the output in $\mathbf{Game}_A$, Simulator B terminates and outputs 0, in case of event **Ev**:

$$\begin{aligned}\Pr[\mathbf{Game}_B] &= \Pr[\mathbf{Game}_B|\mathbf{Ev}]\Pr[\mathbf{Ev}] + \Pr[\mathbf{Game}_B|\neg\mathbf{Ev}]\Pr[\neg\mathbf{Ev}]\\ &= 0 \times \Pr[\mathbf{Ev}] + \Pr[\mathbf{Game}_A|\neg\mathbf{Ev}] \times \Pr[\neg\mathbf{Ev}]\\ &= \Pr[\mathbf{Game}_A] \times \Pr[\neg\mathbf{Ev}]\end{aligned}$$

    Simulator B terminates and flips a coin, in case of event **Ev**:

$$\begin{aligned}\Pr[\mathbf{Game}_B] &= \Pr[\mathbf{Game}_B|\mathbf{Ev}]\Pr[\mathbf{Ev}] + \Pr[\mathbf{Game}_B|\neg\mathbf{Ev}]\Pr[\neg\mathbf{Ev}]\\ &= \tfrac{1}{2} \times \Pr[\mathbf{Ev}] + \Pr[\mathbf{Game}_A|\neg\mathbf{Ev}] \times \Pr[\neg\mathbf{Ev}]\\ &= \tfrac{1}{2} + (\Pr[\mathbf{Game}_A] - \tfrac{1}{2}) \times \Pr[\neg\mathbf{Ev}]\end{aligned}$$

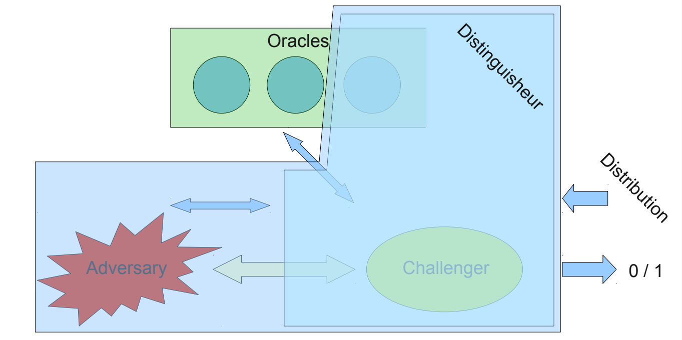
# Two Simulations

- Identical behaviors: $\Pr[\mathbf{Game}_A] - \Pr[\mathbf{Game}_B] = 0$
- The behaviors differ only if **Ev** happens:
  - **Ev** is negligible, one can ignore it
  - **Ev** is non-negligible and independent of the output in $\mathbf{Game}_A$, Simulator B terminates in case of event **Ev**

## Event Ev

- Either **Ev** is negligible, or the output is independent of **Ev**
- For being able to terminate simulation B in case of event **Ev**, this event must be *efficiently* detectable
- For evaluating $\Pr[\mathbf{Ev}]$, one re-iterates the above process, with an initial game that outputs 1 when event **Ev** happens

# Two Distributions




$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] \leq \mathbf{Adv}(\mathcal{D}^{\text{oracles}})$$

# Two Distributions

$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] \leq \mathbf{Adv}(\mathcal{D}^{\text{oracles}})$$

- For identical/statistically close distributions, for any oracle:

$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] = \textbf{Dist}(\textbf{Distrib}_A, \textbf{Distrib}_B) = \text{negl}()$$

- For computationally close distributions, in general, we need to exclude additional oracle access:

$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] \leq \mathbf{Adv}^{\textbf{Distrib}}(t)$$

where $t$ is the computational time of the distinguisheur

## Two Distributions

$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] \leq \mathbf{Adv}(\mathcal{D}^{\text{oracles}})$$

- For identical/statistically close distributions, for any oracle:

$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] = \textbf{Dist}(\textbf{Distrib}_A, \textbf{Distrib}_B) = \text{negl}()$$

- For computationally close distributions, in general, we need to exclude additional oracle access:

$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] \leq \mathbf{Adv}^{\textbf{Distrib}}(t)$$

where $t$ is the computational time of the distinguisheur

# Two Distributions

$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] \leq \mathbf{Adv}(\mathcal{D}^{\text{oracles}})$$

- For identical/statistically close distributions, for any oracle:

$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] = \textbf{Dist}(\textbf{Distrib}_A, \textbf{Distrib}_B) = \text{negl}()$$

- For computationally close distributions, in general, we need to exclude additional oracle access:

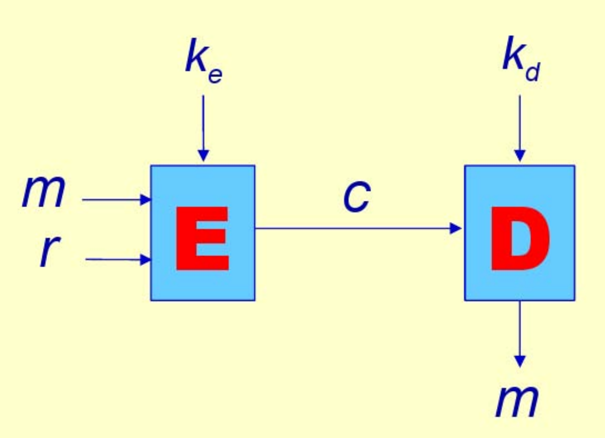
$$\Pr[\textbf{Game}_A] - \Pr[\textbf{Game}_B] \leq \mathbf{Adv}^{\textbf{Distrib}}(t)$$

where $t$ is the computational time of the distinguisheur

# Advanced Security for Encryption

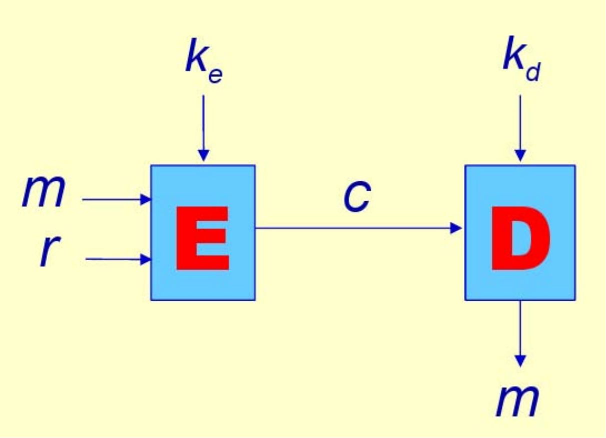
# Outline

## Public-Key Encryption



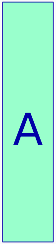

Goal: Privacy/Secrecy of the plaintext

# Public-Key Encryption

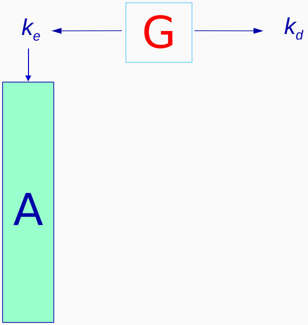



Goal: Privacy/Secrecy of the plaintext

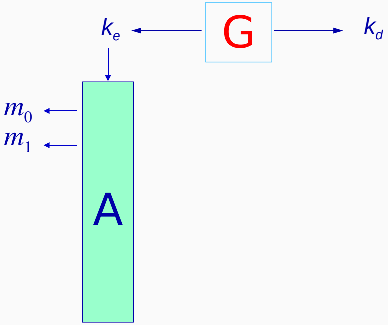
# IND − CPA Security Game



# IND − CPA Security Game

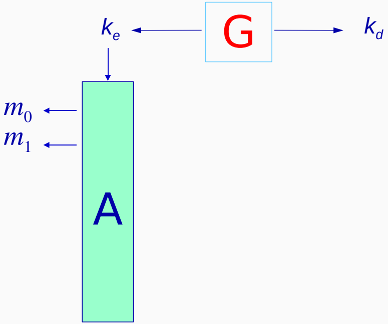


# $\mathrm{IND}-\mathrm{CPA}$ Security Game

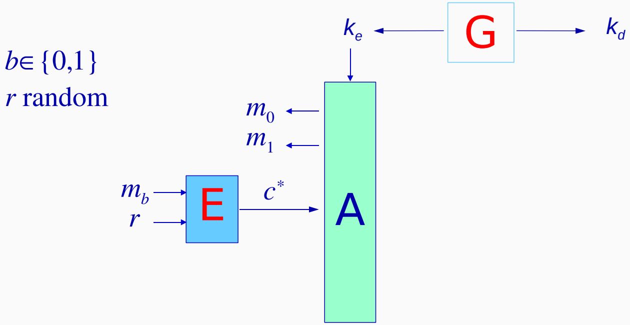


# IND – CPA Security Game

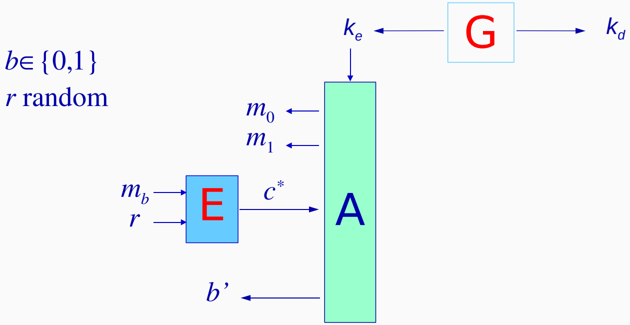
$b \in \{0,1\}$
$r$ random



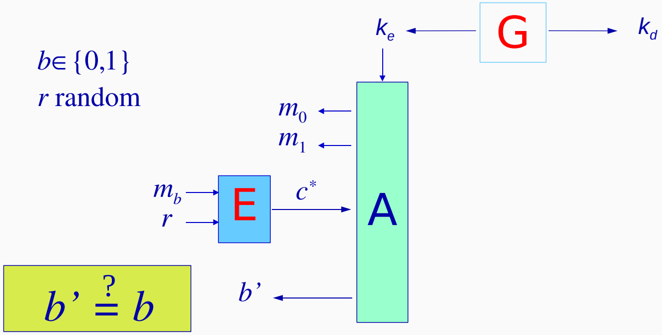
# IND − CPA Security Game



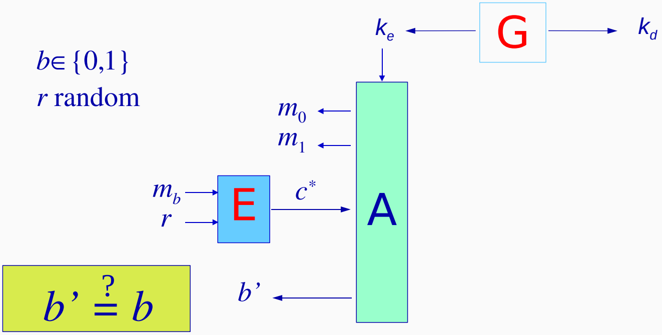
# IND – CPA Security Game



# IND − CPA Security Game



# IND − CPA Security Game




The adversary cannot get any information about a plaintext of a specific ciphertext (validity, partial value, etc)

# Malleability

Semantic security (ciphertext indistinguishability) guarantees that no information is leaked from $c$ about the plaintext $m$

But it may be possible to derive a ciphertext $c'$
such that the plaintext $m'$ is related to $m$ in a meaningful way:

- ElGamal ciphertext: $c_1 = g^r$ and $c_2 = m \times y^r$
- Malleability: $c'_1 = c_1 = g^r$ and $c'_2 = 2 \times c_2 = (2m) \times y^r$

From an encryption of $m$, one can build an encryption of $2m$, or a random ciphertext of $m$, etc.

# Malleability

Semantic security (ciphertext indistinguishability) guarantees that no information is leaked from $c$ about the plaintext $m$

But it may be possible to derive a ciphertext $c'$
such that the plaintext $m'$ is related to $m$ in a meaningful way:

- ElGamal ciphertext: $c_1 = g^r$ and $c_2 = m \times y^r$
- Malleability: $c'_1 = c_1 = g^r$ and $c'_2 = 2 \times c_2 = (2m) \times y^r$

From an encryption of $m$, one can build an encryption of $2m$, or a random ciphertext of $m$, etc.

# Malleability

Semantic security (ciphertext indistinguishability) guarantees that no information is leaked from $c$ about the plaintext $m$

But it may be possible to derive a ciphertext $c'$
such that the plaintext $m'$ is related to $m$ in a meaningful way:

- ElGamal ciphertext: $c_1 = g^r$ and $c_2 = m \times y^r$
- Malleability: $c'_1 = c_1 = g^r$ and $c'_2 = 2 \times c_2 = (2m) \times y^r$

From an encryption of $m$, one can build an encryption of $2m$, or a random ciphertext of $m$, etc.

# Malleability

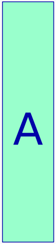
Semantic security (ciphertext indistinguishability) guarantees that no information is leaked from $c$ about the plaintext $m$

But it may be possible to derive a ciphertext $c'$
such that the plaintext $m'$ is related to $m$ in a meaningful way:

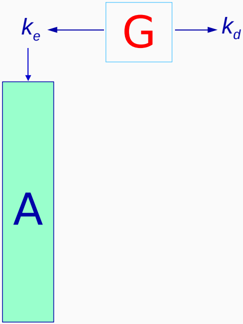
- ElGamal ciphertext: $c_1 = g^r$ and $c_2 = m \times y^r$
- Malleability: $c'_1 = c_1 = g^r$ and $c'_2 = 2 \times c_2 = (2m) \times y^r$

From an encryption of $m$, one can build an encryption of $2m$, or a random ciphertext of $m$, etc.

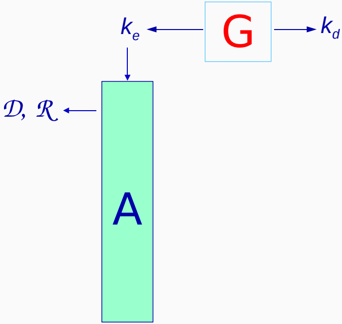
# Non-Malleability: $\mathsf{NM}-\mathsf{CPA}$ Security Game



# Non-Malleability: $\mathrm{NM} - \mathrm{CPA}$ Security Game



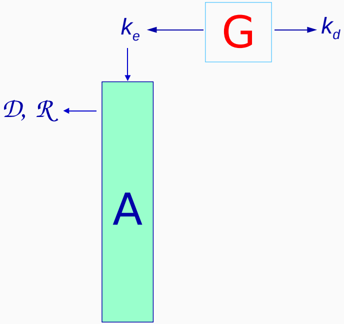
# Non-Malleability: $\mathrm{NM} - \mathrm{CPA}$ Security Game



# Non-Malleability: $\mathrm{NM} - \mathrm{CPA}$ Security Game

$m^*, m' \leftarrow \mathcal{D}$

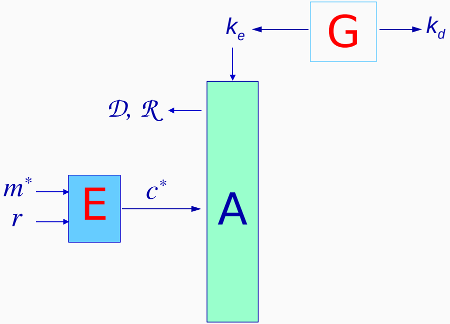
$r$ random



# Non-Malleability: $\mathrm{NM} - \mathrm{CPA}$ Security Game

$m^*, m' \leftarrow \mathcal{D}$

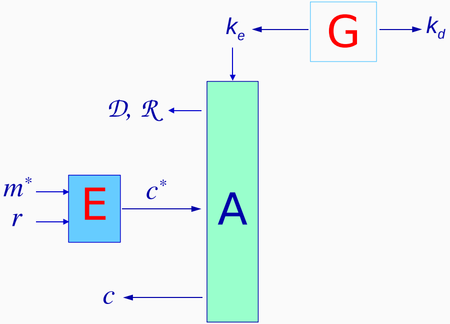
$r$ random



# Non-Malleability: $\mathrm{NM} - \mathrm{CPA}$ Security Game

$m^*, m' \leftarrow \mathcal{D}$

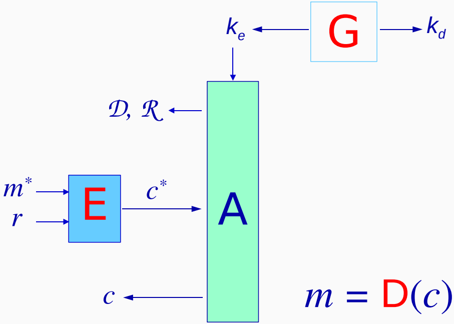
$r$ random



# Non-Malleability: $\mathrm{NM} - \mathrm{CPA}$ Security Game

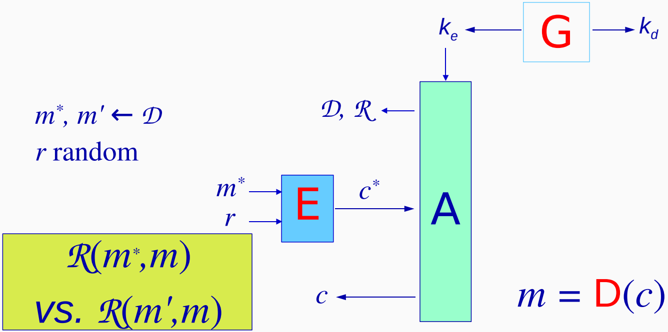
$m^*, m' \leftarrow \mathcal{D}$

$r$ random

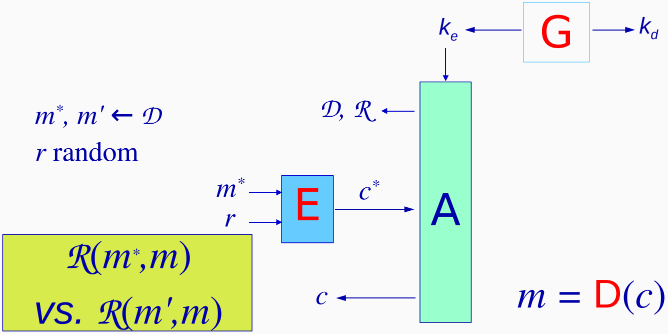



$m = \mathsf{D}(c)$

# Non-Malleability: NM − CPA Security Game



# Non-Malleability: NM − CPA Security Game




$$\mathbf{Adv}_{\mathcal{S}}^{\mathsf{nm-cpa}}(\mathcal{A}) = \left|\Pr[\mathcal{R}(m^*, m)] - \Pr[\mathcal{R}(m', m)]\right|$$

# Additional Information

More information modelled by oracle access

- reaction attacks: oracle which answers, on $c$, whether the ciphertext $c$ is valid or not
- plaintext-checking attacks: oracle which answers, on a pair $(m, c)$, whether the plaintext $m$ is really encrypted in $c$ or not (whether $m = \mathcal{D}_{sk}(c)$)
- chosen-ciphertext attacks ($\mathbf{CCA}$): decryption oracle (with the restriction not to use it on the challenge ciphertext) $\Longrightarrow$ the adversary can obtain the plaintext of any ciphertext of its choice (excepted the challenge)
  - non-adaptive ($\mathbf{CCA}-1$) [Naor-Yung STOC '90] only before receiving the challenge
  - adaptive ($\mathbf{CCA}-2$) [Rackoff-Simon Crypto '91] unlimited oracle access

# Additional Information

More information modelled by oracle access

- reaction attacks: oracle which answers, on $c$, whether the ciphertext $c$ is valid or not
- plaintext-checking attacks: oracle which answers, on a pair $(m, c)$, whether the plaintext $m$ is really encrypted in $c$ or not (whether $m = \mathcal{D}_{sk}(c)$)
- chosen-ciphertext attacks ($\mathbf{CCA}$): decryption oracle (with the restriction not to use it on the challenge ciphertext) $\Longrightarrow$ the adversary can obtain the plaintext of any ciphertext of its choice (excepted the challenge)
  - non-adaptive ($\mathbf{CCA}-1$) [Naor-Yung – STOC '90]
    only before receiving the challenge
  - adaptive ($\mathbf{CCA}-2$) [Rackoff-Simon – Crypto '91]
    unlimited oracle access

# Additional Information

More information modelled by oracle access

- reaction attacks: oracle which answers, on $c$,
  whether the ciphertext $c$ is valid or not
- plaintext-checking attacks: oracle which answers,
  on a pair $(m, c)$, whether the plaintext $m$ is really encrypted in $c$
  or not (whether $m = \mathcal{D}_{sk}(c)$)
- chosen-ciphertext attacks ($\mathbf{CCA}$): decryption oracle
  (with the restriction not to use it on the challenge ciphertext)
  $\Longrightarrow$ the adversary can obtain the plaintext of any ciphertext of its choice (excepted the challenge)
  - non-adaptive ($\mathbf{CCA}-1$) [Naor-Yung – STOC '90]
    only before receiving the challenge
  - adaptive ($\mathbf{CCA}-2$) [Rackoff-Simon – Crypto '91]
    unlimited oracle access

# Additional Information

More information modelled by oracle access

- reaction attacks: oracle which answers, on $c$, whether the ciphertext $c$ is valid or not
- plaintext-checking attacks: oracle which answers, on a pair $(m, c)$, whether the plaintext $m$ is really encrypted in $c$ or not (whether $m = \mathcal{D}_{sk}(c)$)
- chosen-ciphertext attacks ($\mathbf{CCA}$): decryption oracle (with the restriction not to use it on the challenge ciphertext) $\Longrightarrow$ the adversary can obtain the plaintext of any ciphertext of its choice (excepted the challenge)
  - non-adaptive ($\mathbf{CCA} - 1$) [Naor-Yung – STOC '90]
    only before receiving the challenge
  - adaptive ($\mathbf{CCA} - 2$) [Rackoff-Simon – Crypto '91]
    unlimited oracle access

# Additional Information

More information modelled by oracle access

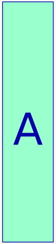
- reaction attacks: oracle which answers, on $c$, whether the ciphertext $c$ is valid or not
- plaintext-checking attacks: oracle which answers, on a pair $(m, c)$, whether the plaintext $m$ is really encrypted in $c$ or not (whether $m = \mathcal{D}_{sk}(c)$)
- chosen-ciphertext attacks ($\mathbf{CCA}$): decryption oracle (with the restriction not to use it on the challenge ciphertext) $\Longrightarrow$ the adversary can obtain the plaintext of any ciphertext of its choice (excepted the challenge)
  - non-adaptive ($\mathbf{CCA} - 1$) [Naor-Yung – STOC '90]
    only before receiving the challenge
  - adaptive ($\mathbf{CCA} - 2$) [Rackoff-Simon – Crypto '91]
    unlimited oracle access

# Additional Information

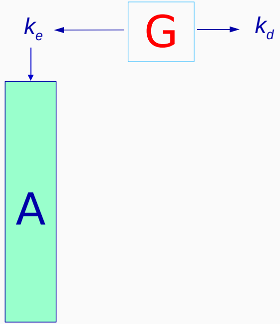
More information modelled by oracle access

- reaction attacks: oracle which answers, on $c$, whether the ciphertext $c$ is valid or not
- plaintext-checking attacks: oracle which answers, on a pair $(m, c)$, whether the plaintext $m$ is really encrypted in $c$ or not (whether $m = \mathcal{D}_{sk}(c)$)
- chosen-ciphertext attacks ($\mathbf{CCA}$): decryption oracle (with the restriction not to use it on the challenge ciphertext) $\Longrightarrow$ the adversary can obtain the plaintext of any ciphertext of its choice (excepted the challenge)
  - non-adaptive ($\mathbf{CCA}-1$) [Naor-Yung – STOC '90]
    only before receiving the challenge
  - adaptive ($\mathbf{CCA}-2$) [Rackoff-Simon – Crypto '91]
    unlimited oracle access

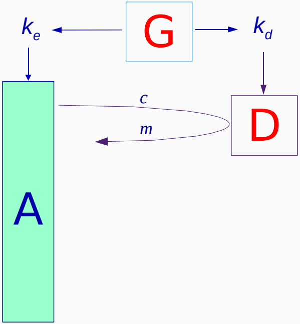
# $\mathbf{IND-CCA}$ Security Game



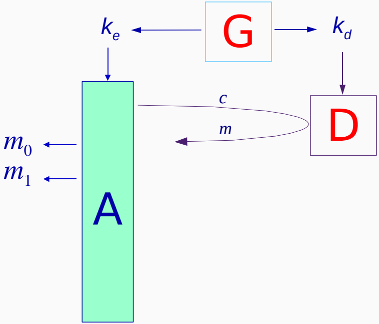
# $\mathrm{IND}-\mathrm{CCA}$ Security Game



# $\mathbf{IND-CCA}$ Security Game

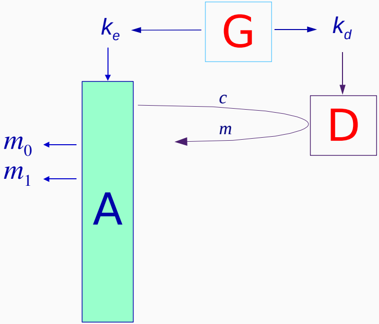


# $\mathrm{IND} - \mathrm{CCA}$ Security Game



# IND − CCA Security Game

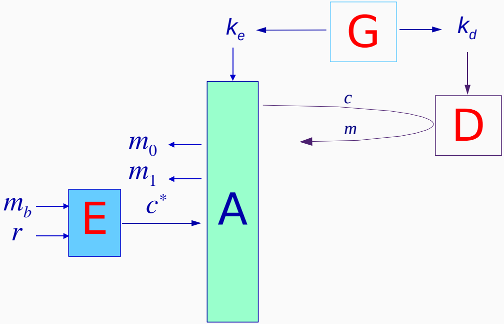
$b \in \{0,1\}$
$r$ random



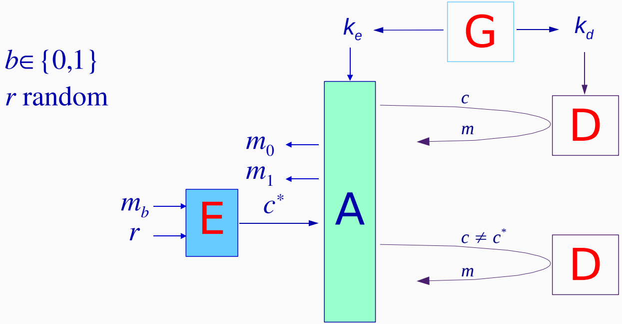
# IND − CCA Security Game

$b \in \{0,1\}$

$r$ random

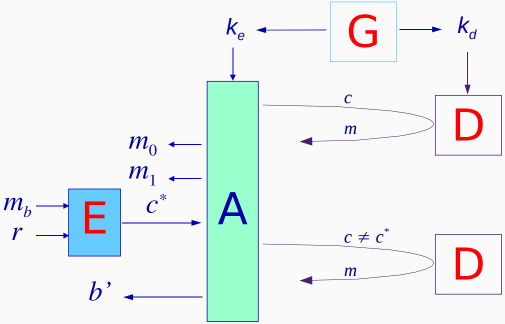


# IND − CCA Security Game

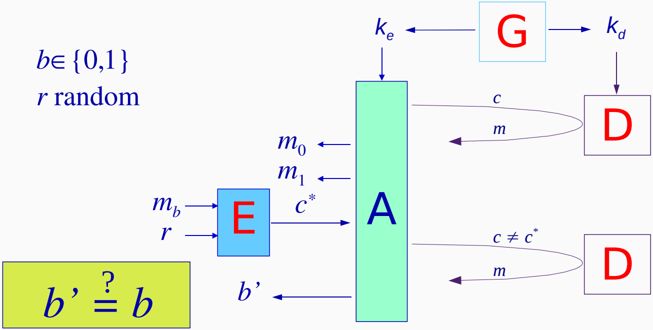


# IND − CCA Security Game

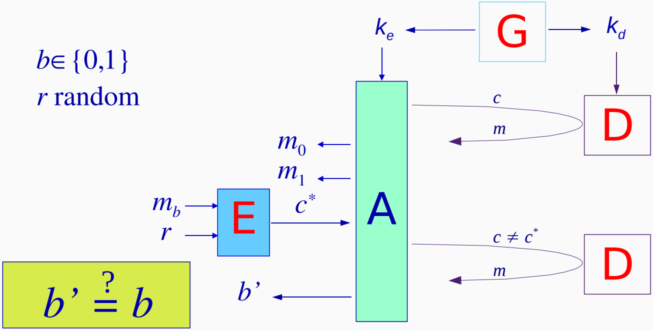
$b \in \{0,1\}$
$r$ random



# IND − CCA Security Game



# $\mathbf{IND-CCA}$ Security Game




The adversary can ask any decryption of its choice:

Chosen-Ciphertext Attacks (oracle access)

$$(sk, pk) \leftarrow \mathcal{K}(); (m_0, m_1, \text{state}) \leftarrow \mathcal{A}^{\mathcal{D}}(pk);$$
$$b \stackrel{R}{\leftarrow} \{0,1\}; c = \mathcal{E}_{pk}(m_b); b' \leftarrow \mathcal{A}^{\mathcal{D}}(\text{state}, c)$$

$$\mathbf{Adv}_{\mathcal{S}}^{\text{ind}-\text{cca}}(\mathcal{A}) = \left|\Pr[b' = 1 | b = 1] - \Pr[b' = 1 | b = 0]\right| = \left|2 \times \Pr[b' = b] - 1\right|$$

$$\begin{array}{ccccc}
\text{NM-CPA} & \Leftarrow & \text{NM-CCA1} & \Leftarrow & \text{NM-CCA2} \\
\Downarrow & & \Downarrow & & \Updownarrow \\
\text{IND-CPA} & \Leftarrow & \text{IND-CCA1} & \Leftarrow & \text{IND-CCA2} \\
\Downarrow & & & & \\
\text{OW-CPA} & & & &
\end{array}$$

minimal security

strong security: CCA

weak security

# Outline

Basic Security Notions

Game-based Proofs

**Advanced Security for Encryption**

- Advanced Security Notions
- Cramer-Shoup Encryption Scheme
- Generic Conversion

Conclusion

# Cramer-Shoup Encryption Scheme

## Key Generation

- $\mathbb{G} = (\langle g \rangle, \times)$ group of order $q$
- $sk = (x_1, x_2, y_1, y_2, z)$, where $x_1, x_2, y_1, y_2, z \stackrel{R}{\leftarrow} \mathbb{Z}_q$
- $pk = (g_1, g_2, \mathcal{H}, c, d, h)$, where
  - $g_1$, $g_2$ are independent elements in $\mathbb{G}$
  - $\mathcal{H}$ a hash function (second-preimage resistant)
  - $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^z$

## Encryption

$u_1 = g_1^r,\ u_2 = g_2^r,\ e = m \times h^r,\ v = c^r d^{r\alpha}$ where $\alpha = \mathcal{H}(u_1, u_2, e)$

# Cramer-Shoup Encryption Scheme

[Cramer-Shoup – Crypto ’98]

## Key Generation

- $\mathbb{G} = (\langle g \rangle, \times)$ group of order $q$
- $sk = (x_1, x_2, y_1, y_2, z)$, where $x_1, x_2, y_1, y_2, z \overset{R}{\leftarrow} \mathbb{Z}_q$
- $pk = (g_1, g_2, \mathcal{H}, c, d, h)$, where
  - $g_1$, $g_2$ are independent elements in $\mathbb{G}$
  - $\mathcal{H}$ a hash function (second-preimage resistant)
  - $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^z$

## Encryption

$$u_1 = g_1^r,\ u_2 = g_2^r,\ e = m \times h^r,\ v = c^r d^{r\alpha} \text{ where } \alpha = \mathcal{H}(u_1, u_2, e)$$

# Cramer-Shoup Encryption Scheme vs. ElGamal

$$u_1 = g_1^r,\ u_2 = g_2^r,\ e = m \times h^r,\ v = c^r d^{r\alpha} \text{ where } \alpha = \mathcal{H}(u_1, u_2, e)$$

$(u_1, e)$ is an ElGamal ciphertext, with public key $h = g_1^z$

**Decryption**

- since $h = g_1^z$, $h^r = u_1^z$, thus $m = e/u_1^z$
- since $c = g_1^{x_1} g_2^{x_2}$ and $d = g_1^{y_1} g_2^{y_2}$

$$c^r = g_1^{rx_1} g_2^{rx_2} = u_1^{x_1} u_2^{x_2} \quad d^r = u_1^{y_1} u_2^{y_2}$$

One thus first checks whether

$$v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2} \text{ where } \alpha = \mathcal{H}(u_1, u_2, e)$$

# Security of the Cramer-Shoup Encryption Scheme

## Theorem

*The Cramer-Shoup encryption scheme achieves* $\mathbf{IND-CCA}$ *security, under the* ***DDH*** *assumption, and the second-preimage resistance of* $\mathcal{H}$*:*

$$\mathbf{Adv}_{\mathcal{CS}}^{\mathsf{ind-cca}}(t) \leq 2 \times \mathbf{Adv}_{\mathbb{G}}^{\mathbf{ddh}}(t) + \mathbf{Succ}^{\mathcal{H}}(t) + 3q_D/q$$

Let us prove this theorem, with a sequence of games, in which $\mathcal{A}$ is an $\mathbf{IND-CCA}$ adversary against the Cramer-Shoup encryption scheme.

# Security of the Cramer-Shoup Encryption Scheme

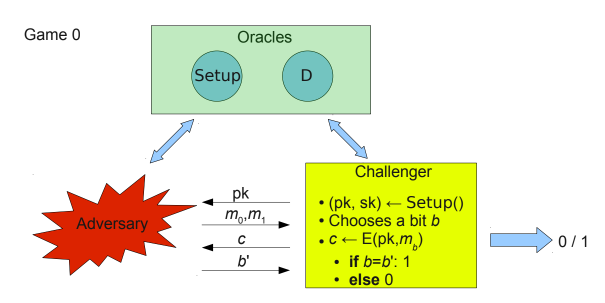
**Theorem**

*The Cramer-Shoup encryption scheme achieves* $\mathbf{IND-CCA}$ *security, under the* ***DDH*** *assumption, and the second-preimage resistance of* $\mathcal{H}$*:*

$$\mathbf{Adv}^{\mathsf{ind-cca}}_{\mathcal{CS}}(t) \leq 2 \times \mathbf{Adv}^{\mathbf{ddh}}_{\mathbb{G}}(t) + \mathbf{Succ}^{\mathcal{H}}(t) + 3q_D/q$$

Let us prove this theorem, with a sequence of games, in which $\mathcal{A}$ is an $\mathbf{IND-CCA}$ adversary against the Cramer-Shoup encryption scheme.

# Real Attack Game




## Key Generation Oracle

$x_1, x_2, y_1, y_2, z \stackrel{R}{\leftarrow} \mathbb{Z}_q$, $g_1, g_2 \stackrel{R}{\leftarrow} \mathbb{G}$: $sk = (x_1, x_2, y_1, y_2, z)$
$c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^z$: $pk = (g_1, g_2, \mathcal{H}, c, d, h)$

## Decryption Oracle

If $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$ where $\alpha = \mathcal{H}(u_1, u_2, e)$: $m = e/u_1^z$

# Proof: Invalid ciphertexts

- **Game**$_0$: use of the oracles $\mathcal{K}$, $\mathcal{D}$
- **Game**$_1$: we abort (with a random output $b'$) in case of bad (invalid) accepted ciphertext, where invalid ciphertext means $\log_{g_1} u_1 \neq \log_{g_2} u_2$

**Event F**

$\mathcal{A}$ submits a bad accepted ciphertext

(note: this is not computationally detectable)

The advantage in **Game**$_1$ is: $\Pr_1[b' = b|\mathbf{F}] = 1/2$

$$\Pr_{\mathbf{Game}_0}[\mathbf{F}] = \Pr_{\mathbf{Game}_1}[\mathbf{F}] \qquad \Pr_{\mathbf{Game}_1}[b' = b|\neg\mathbf{F}] = \Pr_{\mathbf{Game}_0}[b' = b|\neg\mathbf{F}]$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - \Pr[\mathbf{F}]$

# Proof: Invalid ciphertexts

- **Game**$_0$: use of the oracles $\mathcal{K}$, $\mathcal{D}$
- **Game**$_1$: we abort (with a random output $b'$)
  in case of bad (invalid) accepted ciphertext,
  where invalid ciphertext means $\log_{g_1} u_1 \neq \log_{g_2} u_2$

**Event F**

$\mathcal{A}$ submits a bad accepted ciphertext
(note: this is not computationally detectable)

The advantage in **Game**$_1$ is: $\Pr_1[b' = b | \mathbf{F}] = 1/2$

$$\Pr_{\mathbf{Game}_0}[\mathbf{F}] = \Pr_{\mathbf{Game}_1}[\mathbf{F}] \qquad \Pr_{\mathbf{Game}_1}[b' = b | \neg\mathbf{F}] = \Pr_{\mathbf{Game}_0}[b' = b | \neg\mathbf{F}]$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - \Pr[\mathbf{F}]$

# Proof: Invalid ciphertexts

- **Game**$_0$: use of the oracles $\mathcal{K}$, $\mathcal{D}$
- **Game**$_1$: we abort (with a random output $b'$)
  in case of bad (invalid) accepted ciphertext,
  where invalid ciphertext means $\log_{g_1} u_1 \neq \log_{g_2} u_2$

**Event F**

$\mathcal{A}$ submits a bad accepted ciphertext
(note: this is not computationally detectable)

The advantage in **Game**$_1$ is: $\Pr_1[b' = b|\mathbf{F}] = 1/2$

$$\Pr_{\mathbf{Game}_0}[\mathbf{F}] = \Pr_{\mathbf{Game}_1}[\mathbf{F}] \qquad \Pr_{\mathbf{Game}_1}[b' = b|\neg\mathbf{F}] = \Pr_{\mathbf{Game}_0}[b' = b|\neg\mathbf{F}]$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - \Pr[\mathbf{F}]$

# Proof: Invalid ciphertexts

- **Game$_0$**: use of the oracles $\mathcal{K}$, $\mathcal{D}$
- **Game$_1$**: we abort (with a random output $b'$)
  in case of bad (invalid) accepted ciphertext,
  where invalid ciphertext means $\log_{g_1} u_1 \neq \log_{g_2} u_2$

**Event F**

$\mathcal{A}$ submits a bad accepted ciphertext
(note: this is not computationally detectable)

The advantage in **Game$_1$** is: $\Pr_1[b' = b | \mathbf{F}] = 1/2$

$$\Pr_{\mathbf{Game}_0}[\mathbf{F}] = \Pr_{\mathbf{Game}_1}[\mathbf{F}] \qquad \Pr_{\mathbf{Game}_1}[b' = b | \neg\mathbf{F}] = \Pr_{\mathbf{Game}_0}[b' = b | \neg\mathbf{F}]$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - \Pr[\mathbf{F}]$

# Details: Shoup's Lemma

$$\mathbf{Adv}_{\textsf{Game}_1} \quad = \quad 2 \times \Pr_{\textsf{Game}_1}[b' = b] - 1$$

# Details: Shoup's Lemma

$$
\begin{aligned}
\mathbf{Adv}_{\textsf{Game}_1} &= 2 \times \Pr_{\textsf{Game}_1}[b' = b] - 1 \\
&= 2 \times \Pr_{\textsf{Game}_1}[b' = b | \neg \mathbf{F}] \Pr_{\textsf{Game}_1}[\neg \mathbf{F}] \\
&\quad + 2 \times \Pr_{\textsf{Game}_1}[b' = b | \mathbf{F}] \Pr_{\textsf{Game}_1}[\mathbf{F}] - 1
\end{aligned}
$$

# Details: Shoup's Lemma

$$
\begin{aligned}
\mathbf{Adv}_{\textbf{Game}_1} &= 2 \times \Pr_{\textbf{Game}_1}[b' = b] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_1}[b' = b | \neg \mathbf{F}] \Pr_{\textbf{Game}_1}[\neg \mathbf{F}] \\
&\quad + 2 \times \Pr_{\textbf{Game}_1}[b' = b | \mathbf{F}] \Pr_{\textbf{Game}_1}[\mathbf{F}] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_0}[b' = b | \neg \mathbf{F}] \Pr_{\textbf{Game}_0}[\neg \mathbf{F}] + \Pr_{\textbf{Game}_0}[\mathbf{F}] - 1
\end{aligned}
$$

# Details: Shoup's Lemma

$$
\begin{aligned}
\mathbf{Adv}_{\textbf{Game}_1} &= 2 \times \Pr_{\textbf{Game}_1}[b' = b] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_1}[b' = b | \neg \mathbf{F}] \Pr_{\textbf{Game}_1}[\neg \mathbf{F}] \\
&\quad + 2 \times \Pr_{\textbf{Game}_1}[b' = b | \mathbf{F}] \Pr_{\textbf{Game}_1}[\mathbf{F}] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_0}[b' = b | \neg \mathbf{F}] \Pr_{\textbf{Game}_0}[\neg \mathbf{F}] + \Pr_{\textbf{Game}_0}[\mathbf{F}] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_0}[b' = b] - 2 \times \Pr_{\textbf{Game}_0}[b' = b | \mathbf{F}] \Pr_{\textbf{Game}_0}[\mathbf{F}] \\
&\quad + \Pr_{\textbf{Game}_0}[\mathbf{F}] - 1
\end{aligned}
$$

# Details: Shoup's Lemma

$$
\begin{aligned}
\mathbf{Adv}_{\textbf{Game}_1} &= 2 \times \Pr_{\textbf{Game}_1}[b' = b] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_1}[b' = b | \neg \mathbf{F}] \Pr_{\textbf{Game}_1}[\neg \mathbf{F}] \\
&\quad + 2 \times \Pr_{\textbf{Game}_1}[b' = b | \mathbf{F}] \Pr_{\textbf{Game}_1}[\mathbf{F}] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_0}[b' = b | \neg \mathbf{F}] \Pr_{\textbf{Game}_0}[\neg \mathbf{F}] + \Pr_{\textbf{Game}_0}[\mathbf{F}] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_0}[b' = b] - 2 \times \Pr_{\textbf{Game}_0}[b' = b | \mathbf{F}] \Pr_{\textbf{Game}_0}[\mathbf{F}] \\
&\quad + \Pr_{\textbf{Game}_0}[\mathbf{F}] - 1 \\
&= \mathbf{Adv}_{\textbf{Game}_0} - \Pr_{\textbf{Game}_0}[\mathbf{F}] (2 \times \Pr_{\textbf{Game}_0}[b' = b | \mathbf{F}] - 1)
\end{aligned}
$$

## Details: Shoup's Lemma

$$\begin{aligned}
\mathbf{Adv}_{\textbf{Game}_1} &= 2 \times \Pr_{\textbf{Game}_1}[b' = b] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_1}[b' = b | \neg\mathbf{F}] \Pr_{\textbf{Game}_1}[\neg\mathbf{F}] \\
&\quad +2 \times \Pr_{\textbf{Game}_1}[b' = b | \mathbf{F}] \Pr_{\textbf{Game}_1}[\mathbf{F}] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_0}[b' = b | \neg\mathbf{F}] \Pr_{\textbf{Game}_0}[\neg\mathbf{F}] + \Pr_{\textbf{Game}_0}[\mathbf{F}] - 1 \\
&= 2 \times \Pr_{\textbf{Game}_0}[b' = b] - 2 \times \Pr_{\textbf{Game}_0}[b' = b | \mathbf{F}] \Pr_{\textbf{Game}_0}[\mathbf{F}] \\
&\quad + \Pr_{\textbf{Game}_0}[\mathbf{F}] - 1 \\
&= \mathbf{Adv}_{\textbf{Game}_0} - \Pr_{\textbf{Game}_0}[\mathbf{F}](2 \times \Pr_{\textbf{Game}_0}[b' = b | \mathbf{F}] - 1) \\
&\geq \mathbf{Adv}_{\textbf{Game}_0} - \Pr_{\textbf{Game}_0}[\mathbf{F}]
\end{aligned}$$

# Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}]$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$

The adversary just knows the public key:

$$c = g_1^{x_1} g_2^{x_2} \qquad d = g_1^{y_1} g_2^{y_2}$$

Let us move to the exponents, in basis $g_1$, with $g_2 = g_1^s$:

$$\begin{aligned}\log c &= x_1 + s x_2 \\ \log d &= y_1 + s y_2 \\ \log v &= r_1(x_1 + \alpha y_1) + s r_2(x_2 + \alpha y_2)\end{aligned}$$

The system is under-defined: for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system $\Longrightarrow v$ is unpredictable

$\Longrightarrow \Pr[\mathbf{F}] \leq q_D/q \qquad \Longrightarrow \mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - q_D/q$

# Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}]$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$

The adversary just knows the public key:

$$c = g_1^{x_1} g_2^{x_2} \qquad d = g_1^{y_1} g_2^{y_2}$$

Let us move to the exponents, in basis $g_1$, with $g_2 = g_1^s$:

$$\begin{aligned} \log c &= x_1 + sx_2 \\ \log d &= y_1 + sy_2 \\ \log v &= r_1(x_1 + \alpha y_1) + sr_2(x_2 + \alpha y_2) \end{aligned}$$

The system is under-defined: for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system $\implies v$ is unpredictable

$\implies \Pr[\mathbf{F}] \leq q_D/q \qquad \implies \mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - q_D/q$

# Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}]$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$

The adversary just knows the public key:

$$c = g_1^{x_1} g_2^{x_2} \qquad d = g_1^{y_1} g_2^{y_2}$$

Let us move to the exponents, in basis $g_1$, with $g_2 = g_1^s$:

$$\begin{aligned} \log c &= x_1 + s x_2 \\ \log d &= y_1 + s y_2 \\ \log v &= r_1(x_1 + \alpha y_1) + s r_2(x_2 + \alpha y_2) \end{aligned}$$

The system is under-defined: for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system $\implies v$ is unpredictable

$\implies \Pr[\mathbf{F}] \leq q_D/q \qquad \implies \mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - q_D/q$

# Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}]$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$

The adversary just knows the public key:

$$c = g_1^{x_1} g_2^{x_2} \qquad d = g_1^{y_1} g_2^{y_2}$$

Let us move to the exponents, in basis $g_1$, with $g_2 = g_1^s$:

$$\begin{aligned} \log c &= x_1 + s x_2 \\ \log d &= y_1 + s y_2 \\ \log v &= r_1(x_1 + \alpha y_1) + s r_2(x_2 + \alpha y_2) \end{aligned}$$

The system is under-defined: for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system $\Longrightarrow$ $v$ is unpredictable

$\Longrightarrow \Pr[\mathbf{F}] \leq q_D/q \qquad \Longrightarrow \mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - q_D/q$

# Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}]$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$

The adversary just knows the public key:

$$c = g_1^{x_1} g_2^{x_2} \qquad d = g_1^{y_1} g_2^{y_2}$$

Let us move to the exponents, in basis $g_1$, with $g_2 = g_1^s$:

$$\begin{aligned} \log c &= x_1 + s x_2 \\ \log d &= y_1 + s y_2 \\ \log v &= r_1(x_1 + \alpha y_1) + s r_2(x_2 + \alpha y_2) \end{aligned}$$

The system is under-defined: for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system $\implies v$ is unpredictable

$\implies \Pr[\mathbf{F}] \leq q_D/q \qquad \implies \mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - q_D/q$

# Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}]$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$

The adversary just knows the public key:

$$c = g_1^{x_1} g_2^{x_2} \qquad d = g_1^{y_1} g_2^{y_2}$$

Let us move to the exponents, in basis $g_1$, with $g_2 = g_1^s$:

$$\begin{aligned} \log c &= x_1 + s x_2 \\ \log d &= y_1 + s y_2 \\ \log v &= r_1(x_1 + \alpha y_1) + s r_2(x_2 + \alpha y_2) \end{aligned}$$

The system is under-defined: for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system $\implies v$ is unpredictable

$\implies \Pr[\mathbf{F}] \leq q_D/q \qquad \implies \mathbf{Adv}_{\mathbf{Game}_1} \geq \mathbf{Adv}_{\mathbf{Game}_0} - q_D/q$

## Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}]$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$

The adversary just knows the public key:

$$c = g_1^{x_1} g_2^{x_2} \qquad d = g_1^{y_1} g_2^{y_2}$$

Let us move to the exponents, in basis $g_1$, with $g_2 = g_1^s$:

$$\begin{array}{rcl} \log c & = & x_1 + s x_2 \\ \log d & = & y_1 + s y_2 \\ \log v & = & r_1(x_1 + \alpha y_1) + s r_2(x_2 + \alpha y_2) \end{array}$$

The system is under-defined: for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system $\quad \Longrightarrow v$ is unpredictable

$\Longrightarrow \Pr[\mathbf{F}] \leq q_D/q \qquad \Longrightarrow \mathbf{Adv}_{\mathsf{Game}_1} \geq \mathbf{Adv}_{\mathsf{Game}_0} - q_D/q$

# Proof: Simulations

- **Game**$_2$: we use the simulations

**Key Generation Simulation**

$x_1, x_2, y_1, y_2, z_1, z_2 \stackrel{R}{\leftarrow} \mathbb{Z}_q$, $g_1, g_2 \stackrel{R}{\leftarrow} \mathbb{G}$: $sk = (x_1, x_2, y_1, y_2, z_1, z_2)$

$g_2 = g_1^s$

$c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^{z_1} g_2^{z_2}$: $pk = (g_1, g_2, \mathcal{H}, c, d, h)$

$z = z_1 + s z_2$

Distribution of the public key: Identical

**Decryption Simulation**

If $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$ where $\alpha = \mathcal{H}(u_1, u_2, e)$: $m = e/u_1^{z_1} u_2^{z_2}$

Under the assumption of $\neg$**F**, perfect simulation

$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathbf{Game}_2} = \mathbf{Adv}_{\mathbf{Game}_1}$

# Proof: Simulations

- **Game$_2$**: we use the simulations

**Key Generation Simulation**

$x_1, x_2, y_1, y_2, z_1, z_2 \stackrel{R}{\leftarrow} \mathbb{Z}_q$, $g_1, g_2 \stackrel{R}{\leftarrow} \mathbb{G}$: $sk = (x_1, x_2, y_1, y_2, z_1, z_2)$

$g_2 = g_1^s$

$c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^{z_1} g_2^{z_2}$: $pk = (g_1, g_2, \mathcal{H}, c, d, h)$

$z = z_1 + sz_2$

Distribution of the public key: Identical

**Decryption Simulation**

If $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$ where $\alpha = \mathcal{H}(u_1, u_2, e)$: $m = e/u_1^{z_1} u_2^{z_2}$

Under the assumption of $\neg$**F**, perfect simulation

$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathbf{Game}_2} = \mathbf{Adv}_{\mathbf{Game}_1}$

# Proof: Simulations

- **Game$_2$**: we use the simulations

**Key Generation Simulation**

$x_1, x_2, y_1, y_2, z_1, z_2 \stackrel{R}{\leftarrow} \mathbb{Z}_q$, $g_1, g_2 \stackrel{R}{\leftarrow} \mathbb{G}$: $sk = (x_1, x_2, y_1, y_2, z_1, z_2)$

$g_2 = g_1^s$

$c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^{z_1} g_2^{z_2}$: $pk = (g_1, g_2, \mathcal{H}, c, d, h)$

$z = z_1 + sz_2$

Distribution of the public key: Identical

**Decryption Simulation**

If $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$ where $\alpha = \mathcal{H}(u_1, u_2, e)$: $m = e/u_1^{z_1} u_2^{z_2}$

Under the assumption of $\neg$**F**, perfect simulation

$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathbf{Game}_2} = \mathbf{Adv}_{\mathbf{Game}_1}$

# Proof: Simulations

- **Game$_2$**: we use the simulations

### Key Generation Simulation

$x_1, x_2, y_1, y_2, z_1, z_2 \xleftarrow{R} \mathbb{Z}_q$, $g_1, g_2 \xleftarrow{R} \mathbb{G}$: $sk = (x_1, x_2, y_1, y_2, z_1, z_2)$

$g_2 = g_1^s$

$c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^{z_1} g_2^{z_2}$: $pk = (g_1, g_2, \mathcal{H}, c, d, h)$

$z = z_1 + s z_2$

Distribution of the public key: Identical

### Decryption Simulation

If $v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$ where $\alpha = \mathcal{H}(u_1, u_2, e)$: $m = e / u_1^{z_1} u_2^{z_2}$

Under the assumption of $\neg$**F**, perfect simulation

$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathbf{Game}_2} = \mathbf{Adv}_{\mathbf{Game}_1}$

# Proof: Simulations

- **Game**$_2$: we use the simulations

## Key Generation Simulation

$x_1, x_2, y_1, y_2, z_1, z_2 \stackrel{R}{\leftarrow} \mathbb{Z}_q$, $g_1, g_2 \stackrel{R}{\leftarrow} \mathbb{G}$: $sk = (x_1, x_2, y_1, y_2, z_1, z_2)$

$\boxed{g_2 = g_1^s}$

$c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^{z_1} g_2^{z_2}$: $pk = (g_1, g_2, \mathcal{H}, c, d, h)$

$\boxed{z = z_1 + s z_2}$

Distribution of the public key: Identical

## Decryption Simulation

If $v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$ where $\alpha = \mathcal{H}(u_1, u_2, e)$: $m = e / u_1^{z_1} u_2^{z_2}$

Under the assumption of $\neg$**F**, perfect simulation

$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathbf{Game}_2} = \mathbf{Adv}_{\mathbf{Game}_1}$

# Proof: Simulations

- **Game**$_2$: we use the simulations

## Key Generation Simulation

$x_1, x_2, y_1, y_2, z_1, z_2 \stackrel{R}{\leftarrow} \mathbb{Z}_q$, $g_1, g_2 \stackrel{R}{\leftarrow} \mathbb{G}$: $sk = (x_1, x_2, y_1, y_2, z_1, z_2)$

$g_2 = g_1^s$

$c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, and $h = g_1^{z_1} g_2^{z_2}$: $pk = (g_1, g_2, \mathcal{H}, c, d, h)$

$z = z_1 + s z_2$

Distribution of the public key: Identical

## Decryption Simulation

If $v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$ where $\alpha = \mathcal{H}(u_1, u_2, e)$: $m = e / u_1^{z_1} u_2^{z_2}$

Under the assumption of $\neg$**F**, perfect simulation

$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathsf{Game}_2} = \mathbf{Adv}_{\mathsf{Game}_1}$

# Proof: Computable Adversary

- **Game**$_3$: we do no longer exclude bad accepted ciphertexts
  $\Longrightarrow$ **Hop-S-Negl**:
  $\mathbf{Adv}_{\mathsf{Game}_3} \geq \mathbf{Adv}_{\mathsf{Game}_2} - \Pr[\mathsf{F}] \geq \mathbf{Adv}_{\mathsf{Game}_2} - q_D/q$

  This is technical: to make the simulator/adversary computable

## Proof: Computable Adversary

- **Game**$_3$: we do no longer exclude bad accepted ciphertexts
  $\Longrightarrow$ **Hop-S-Negl**:
  $\mathbf{Adv}_{\mathsf{Game}_3} \geq \mathbf{Adv}_{\mathsf{Game}_2} - \Pr[\mathsf{F}] \geq \mathbf{Adv}_{\mathsf{Game}_2} - q_D/q$

  This is technical: to make the simulator/adversary computable

## Proof: Computable Adversary

- **Game**$_3$: we do no longer exclude bad accepted ciphertexts
  $\Longrightarrow$ **Hop-S-Negl**:
  $\mathbf{Adv}_{\textsf{Game}_3} \geq \mathbf{Adv}_{\textsf{Game}_2} - \Pr[\mathbf{F}] \geq \mathbf{Adv}_{\textsf{Game}_2} - q_D/q$

  This is technical: to make the simulator/adversary computable

# Proof: Computable Adversary

- **Game**$_3$: we do no longer exclude bad accepted ciphertexts
  $\Longrightarrow$ **Hop-S-Negl**:
  $\mathbf{Adv}_{\textsf{Game}_3} \geq \mathbf{Adv}_{\textsf{Game}_2} - \Pr[\mathbf{F}] \geq \mathbf{Adv}_{\textsf{Game}_2} - q_D/q$

  This is technical: to make the simulator/adversary computable

# Proof: DDH Assumption

- **Game$_4$**: we modify the generation of the challenge ciphertext:

**Original Challenge**

Random choice: $b \stackrel{R}{\leftarrow} \{0,1\}, r \stackrel{R}{\leftarrow} \mathbb{Z}_q$ $[\alpha = \mathcal{H}(u_1, u_2, e)]$

$$u_1 = g_1^r,\ u_2 = g_2^r,\ e = m_b \times h^r,\ v = c^r d^{r\alpha}$$

**New Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0,1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

With $(U = g_1^r, V = g_2^r)$: $U^{z_1} V^{z_2} = h^r$ and $U^{x_1+\alpha y_1} V^{x_2+\alpha y_2} = c^r d^{r\alpha}$
$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathbf{Game}_4} = \mathbf{Adv}_{\mathbf{Game}_3}$

# Proof: DDH Assumption

- **Game**$_4$: we modify the generation of the challenge ciphertext:

**Original Challenge**

Random choice: $b \stackrel{R}{\leftarrow} \{0, 1\}, r \stackrel{R}{\leftarrow} \mathbb{Z}_q$ $[\alpha = \mathcal{H}(u_1, u_2, e)]$

$$u_1 = g_1^r,\ u_2 = g_2^r,\ e = m_b \times h^r,\ v = c^r d^{r\alpha}$$

**New Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0, 1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

With $(U = g_1^r, V = g_2^r)$: $U^{z_1} V^{z_2} = h^r$ and $U^{x_1+\alpha y_1} V^{x_2+\alpha y_2} = c^r d^{r\alpha}$

$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathbf{Game}_4} = \mathbf{Adv}_{\mathbf{Game}_3}$

# Proof: DDH Assumption

- **Game**$_4$: we modify the generation of the challenge ciphertext:

**Original Challenge**

Random choice: $b \stackrel{R}{\leftarrow} \{0,1\}, r \stackrel{R}{\leftarrow} \mathbb{Z}_q$ $\qquad [\alpha = \mathcal{H}(u_1, u_2, e)]$

$$u_1 = g_1^r,\ u_2 = g_2^r,\ e = m_b \times h^r,\ v = c^r d^{r\alpha}$$

**New Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0,1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

With $(U = g_1^r, V = g_2^r)$: $U^{z_1} V^{z_2} = h^r$ and $U^{x_1+\alpha y_1} V^{x_2+\alpha y_2} = c^r d^{r\alpha}$

$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathbf{Game}_4} = \mathbf{Adv}_{\mathbf{Game}_3}$

# Proof: DDH Assumption

- **Game$_4$**: we modify the generation of the challenge ciphertext:

**Original Challenge**

Random choice: $b \stackrel{R}{\leftarrow} \{0,1\}, r \stackrel{R}{\leftarrow} \mathbb{Z}_q$ $[\alpha = \mathcal{H}(u_1, u_2, e)]$

$$u_1 = g_1^r,\ u_2 = g_2^r,\ e = m_b \times h^r,\ v = c^r d^{r\alpha}$$

**New Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0,1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

With $(U = g_1^r, V = g_2^r)$: $U^{z_1} V^{z_2} = h^r$ and $U^{x_1+\alpha y_1} V^{x_2+\alpha y_2} = c^r d^{r\alpha}$
$\Longrightarrow$ **Hop-S-Perfect**: $\mathrm{Adv}_{\mathbf{Game}_4} = \mathrm{Adv}_{\mathbf{Game}_3}$

# Proof: DDH Assumption

- **Game$_4$**: we modify the generation of the challenge ciphertext:

**Original Challenge**

Random choice: $b \stackrel{R}{\leftarrow} \{0,1\}, r \stackrel{R}{\leftarrow} \mathbb{Z}_q$ $\qquad [\alpha = \mathcal{H}(u_1, u_2, e)]$

$$u_1 = g_1^r,\ u_2 = g_2^r,\ e = m_b \times h^r,\ v = c^r d^{r\alpha}$$

**New Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0,1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

With $(U = g_1^r, V = g_2^r)$: $U^{z_1} V^{z_2} = h^r$ and $U^{x_1+\alpha y_1} V^{x_2+\alpha y_2} = c^r d^{r\alpha}$
$\Longrightarrow$ **Hop-S-Perfect**: $\mathbf{Adv}_{\mathbf{Game}_4} = \mathbf{Adv}_{\mathbf{Game}_3}$

# Proof: DDH Assumption

- **Game$_5$**: we modify the generation of the challenge ciphertext:

**Previous Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0, 1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

**New Challenge 2**

Given $(U = g_1^{r_1}, V = g_2^{r_2})$ and random choice $b \stackrel{R}{\leftarrow} \{0, 1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

The input changes from $(U = g_1^r, V = g_2^r)$ to $(U = g_1^{r_1}, V = g_2^{r_2})$:
$\Longrightarrow$ **Hop-D-Comp**: $\mathbf{Adv}_{\mathbf{Game}_5} \geq \mathbf{Adv}_{\mathbf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\mathbf{ddh}}(t)$

# Proof: DDH Assumption

- **Game**$_5$: we modify the generation of the challenge ciphertext:

**Previous Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0,1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

**New Challenge 2**

Given $(U = g_1^{r_1}, V = g_2^{r_2})$ and random choice $b \stackrel{R}{\leftarrow} \{0,1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

The input changes from $(U = g_1^r, V = g_2^r)$ to $(U = g_1^{r_1}, V = g_2^{r_2})$:

$\Longrightarrow$ **Hop-D-Comp**: $\mathbf{Adv}_{\mathbf{Game}_5} \geq \mathbf{Adv}_{\mathbf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\mathbf{ddh}}(t)$

# Proof: DDH Assumption

- **Game**$_5$: we modify the generation of the challenge ciphertext:

**Previous Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0, 1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

**New Challenge 2**

Given $(U = g_1^{r_1}, V = g_2^{r_2})$ and random choice $b \stackrel{R}{\leftarrow} \{0, 1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

The input changes from $(U = g_1^r, V = g_2^r)$ to $(U = g_1^{r_1}, V = g_2^{r_2})$:

$\Longrightarrow$ **Hop-D-Comp**: $\mathbf{Adv}_{\mathbf{Game}_5} \geq \mathbf{Adv}_{\mathbf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\mathbf{ddh}}(t)$

# Proof: DDH Assumption

- **Game**$_5$: we modify the generation of the challenge ciphertext:

**Previous Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0, 1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1 + \alpha y_1} V^{x_2 + \alpha y_2}$$

**New Challenge 2**

Given $(U = g_1^{r_1}, V = g_2^{r_2})$ and random choice $b \stackrel{R}{\leftarrow} \{0, 1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1 + \alpha y_1} V^{x_2 + \alpha y_2}$$

The input changes from $(U = g_1^r, V = g_2^r)$ to $(U = g_1^{r_1}, V = g_2^{r_2})$:
$\Longrightarrow$ **Hop-D-Comp**: $\mathbf{Adv}_{\mathbf{Game}_5} \geq \mathbf{Adv}_{\mathbf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\mathbf{ddh}}(t)$

# Proof: DDH Assumption

- **Game$_5$**: we modify the generation of the challenge ciphertext:

**Previous Challenge 1**

Given $(U = g_1^r, V = g_2^r)$ and random choice $b \stackrel{R}{\leftarrow} \{0, 1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

**New Challenge 2**

Given $(U = g_1^{r_1}, V = g_2^{r_2})$ and random choice $b \stackrel{R}{\leftarrow} \{0, 1\}$

$$u_1 = U,\ u_2 = V,\ e = m_b \times U^{z_1} V^{z_2},\ v = U^{x_1+\alpha y_1} V^{x_2+\alpha y_2}$$

The input changes from $(U = g_1^r, V = g_2^r)$ to $(U = g_1^{r_1}, V = g_2^{r_2})$:
$\Longrightarrow$ **Hop-D-Comp**: $\mathbf{Adv}_{\mathsf{Game}_5} \geq \mathbf{Adv}_{\mathsf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t)$

## Proof: DDH Assumption

The input from outside changes from ($U = g_1^r, V = g_2^r$) (a CDH tuple) to ($U = g_1^{r_1}, V = g_2^{r_2}$) (a random tuple):

$$\Pr_{\textbf{Game}_4}[b' = b] - \Pr_{\textbf{Game}_5}[b' = b] \leq \mathbf{Adv}_{\mathbb{G}}^{\textbf{ddh}}(t)$$

$\Longrightarrow$ **Hop-D-Comp**: $\mathbf{Adv}_{\textbf{Game}_5} \geq \mathbf{Adv}_{\textbf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\textbf{ddh}}(t)$
(Since $\mathbf{Adv} = 2 \times \Pr[b' = b] - 1$)

# Proof: DDH Assumption

The input from outside changes from $(U = g_1^r, V = g_2^r)$ (a CDH tuple) to $(U = g_1^{r_1}, V = g_2^{r_2})$ (a random tuple):

$$\Pr_{\textbf{Game}_4}[b' = b] - \Pr_{\textbf{Game}_5}[b' = b] \leq \mathbf{Adv}_{\mathbb{G}}^{\textbf{ddh}}(t)$$

$\Longrightarrow$ **Hop-D-Comp**: $\mathbf{Adv}_{\textbf{Game}_5} \geq \mathbf{Adv}_{\textbf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\textbf{ddh}}(t)$
(Since $\mathbf{Adv} = 2 \times \Pr[b' = b] - 1$)

# Proof: DDH Assumption

The input from outside changes from ($U = g_1^r, V = g_2^r$) (a CDH tuple) to ($U = g_1^{r_1}, V = g_2^{r_2}$) (a random tuple):

$$\Pr_{\textbf{Game}_4}[b' = b] - \Pr_{\textbf{Game}_5}[b' = b] \leq \mathbf{Adv}_{\mathbb{G}}^{\textbf{ddh}}(t)$$

$\Longrightarrow$ **Hop-D-Comp**: $\mathbf{Adv}_{\textbf{Game}_5} \geq \mathbf{Adv}_{\textbf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\textbf{ddh}}(t)$
(Since $\mathbf{Adv} = 2 \times \Pr[b' = b] - 1$)

# Proof: DDH Assumption

The input from outside changes from ($U = g_1^r, V = g_2^r$) (a CDH tuple) to ($U = g_1^{r_1}, V = g_2^{r_2}$) (a random tuple):

$$\Pr_{\textbf{Game}_4}[b' = b] - \Pr_{\textbf{Game}_5}[b' = b] \leq \mathbf{Adv}_{\mathbb{G}}^{\textbf{ddh}}(t)$$

$\Longrightarrow$ **Hop-D-Comp**: $\mathbf{Adv}_{\textbf{Game}_5} \geq \mathbf{Adv}_{\textbf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\textbf{ddh}}(t)$
(Since $\mathbf{Adv} = 2 \times \Pr[b' = b] - 1$)

# Proof: Collision

- **Game**$_6$: we abort (with a random output $b'$) in case of second pre-image with a decryption query

**Event F**$_H$

$\mathcal{A}$ submits a ciphertext with the same $\alpha$ as the challenge ciphertext, but a different initial triple: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$, were "*" are for all the elements related to the challenge ciphertext.

Second pre-image of $\mathcal{H}$: $\Longrightarrow \Pr[\mathbf{F}_H] \leq \mathbf{Succ}^{\mathcal{H}}(t)$

The advantage in **Game**$_6$ is: $\Pr_{\mathbf{Game}_6}[b' = b | \mathbf{F}_H] = 1/2$

$$\Pr_{\mathbf{Game}_5}[\mathbf{F}_H] = \Pr_{\mathbf{Game}_6}[\mathbf{F}_H] \qquad \Pr_{\mathbf{Game}_6}[b' = b | \neg\mathbf{F}_H] = \Pr_{\mathbf{Game}_5}[b' = b | \neg\mathbf{F}_H]$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_6} \geq \mathbf{Adv}_{\mathbf{Game}_5} - \Pr[\mathbf{F}_H]$

$$\mathbf{Adv}_{\mathbf{Game}_6} \geq \mathbf{Adv}_{\mathbf{Game}_5} - \mathbf{Succ}^{\mathcal{H}}(t)$$

# Proof: Collision

- **Game$_6$**: we abort (with a random output $b'$)
  in case of second pre-image with a decryption query

**Event $\mathbf{F}_H$**

$\mathcal{A}$ submits a ciphertext with the same $\alpha$ as the challenge ciphertext, but a different initial triple: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$, were "*" are for all the elements related to the challenge ciphertext.

Second pre-image of $\mathcal{H}$: $\Longrightarrow \Pr[\mathbf{F}_H] \leq \mathbf{Succ}^{\mathcal{H}}(t)$

The advantage in **Game$_6$** is: $\Pr_{\mathbf{Game}_6}[b' = b | \mathbf{F}_H] = 1/2$

$$\Pr_{\mathbf{Game}_5}[\mathbf{F}_H] = \Pr_{\mathbf{Game}_6}[\mathbf{F}_H] \qquad \Pr_{\mathbf{Game}_6}[b' = b | \neg\mathbf{F}_H] = \Pr_{\mathbf{Game}_5}[b' = b | \neg\mathbf{F}_H]$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_6} \geq \mathbf{Adv}_{\mathbf{Game}_5} - \Pr[\mathbf{F}_H]$

$$\mathbf{Adv}_{\mathbf{Game}_6} \geq \mathbf{Adv}_{\mathbf{Game}_5} - \mathbf{Succ}^{\mathcal{H}}(t)$$

# Proof: Collision

- **Game$_6$**: we abort (with a random output $b'$) in case of second pre-image with a decryption query

**Event $\mathbf{F}_H$**

$\mathcal{A}$ submits a ciphertext with the same $\alpha$ as the challenge ciphertext, but a different initial triple: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$, were "*" are for all the elements related to the challenge ciphertext.

Second pre-image of $\mathcal{H}$: $\Longrightarrow \Pr[\mathbf{F}_H] \leq \mathbf{Succ}^{\mathcal{H}}(t)$

The advantage in **Game$_6$** is: $\Pr_{\mathbf{Game}_6}[b' = b | \mathbf{F}_H] = 1/2$

$$\Pr_{\mathbf{Game}_5}[\mathbf{F}_H] = \Pr_{\mathbf{Game}_6}[\mathbf{F}_H] \qquad \Pr_{\mathbf{Game}_6}[b' = b | \neg\mathbf{F}_H] = \Pr_{\mathbf{Game}_5}[b' = b | \neg\mathbf{F}_H]$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_6} \geq \mathbf{Adv}_{\mathbf{Game}_5} - \Pr[\mathbf{F}_H]$

$$\mathbf{Adv}_{\mathbf{Game}_6} \geq \mathbf{Adv}_{\mathbf{Game}_5} - \mathbf{Succ}^{\mathcal{H}}(t)$$

# Proof: Collision

- **Game$_6$**: we abort (with a random output $b'$) in case of second pre-image with a decryption query

**Event $\mathbf{F}_H$**

$\mathcal{A}$ submits a ciphertext with the same $\alpha$ as the challenge ciphertext, but a different initial triple: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$, were "*" are for all the elements related to the challenge ciphertext.

Second pre-image of $\mathcal{H}$: $\Longrightarrow \Pr[\mathbf{F}_H] \leq \mathbf{Succ}^{\mathcal{H}}(t)$

The advantage in **Game$_6$** is: $\Pr_{\mathbf{Game}_6}[b' = b | \mathbf{F}_H] = 1/2$

$$\Pr_{\mathbf{Game}_5}[\mathbf{F}_H] = \Pr_{\mathbf{Game}_6}[\mathbf{F}_H] \qquad \Pr_{\mathbf{Game}_6}[b' = b | \neg\mathbf{F}_H] = \Pr_{\mathbf{Game}_5}[b' = b | \neg\mathbf{F}_H]$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_6} \geq \mathbf{Adv}_{\mathbf{Game}_5} - \Pr[\mathbf{F}_H]$

$$\mathbf{Adv}_{\mathbf{Game}_6} \geq \mathbf{Adv}_{\mathbf{Game}_5} - \mathbf{Succ}^{\mathcal{H}}(t)$$

# Proof: Invalid ciphertexts

- **Game**$_7$: we abort (with a random output $b'$)
  in case of bad accepted ciphertext,
  we do as in **Game**$_1$

**Event F**$'$

$\mathcal{A}$ submits a bad accepted ciphertext
(note: this is not computationally detectable)

The advantage in **Game**$_7$ is: $\Pr_{\mathbf{Game}_7}[b' = b | \mathbf{F}'] = 1/2$

$$\Pr_{\mathbf{Game}_6}[\mathbf{F}'] = \Pr_{\mathbf{Game}_7}[\mathbf{F}'] \qquad \Pr_{\mathbf{Game}_7}[b' = b | \neg\mathbf{F}'] = \Pr_{\mathbf{Game}_6}[b' = b | \neg\mathbf{F}']$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_7} \geq \mathbf{Adv}_{\mathbf{Game}_6} - \Pr[\mathbf{F}']$

# Proof: Invalid ciphertexts

- **Game**$_7$: we abort (with a random output $b'$) in case of bad accepted ciphertext, we do as in **Game**$_1$

**Event $\mathbf{F}'$**

$\mathcal{A}$ submits a bad accepted ciphertext
(note: this is not computationally detectable)

The advantage in **Game**$_7$ is: $\Pr_{\mathbf{Game}_7}[b' = b | \mathbf{F}'] = 1/2$

$$\Pr_{\mathbf{Game}_6}[\mathbf{F}'] = \Pr_{\mathbf{Game}_7}[\mathbf{F}'] \qquad \Pr_{\mathbf{Game}_7}[b' = b | \neg\mathbf{F}'] = \Pr_{\mathbf{Game}_6}[b' = b | \neg\mathbf{F}']$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_7} \geq \mathbf{Adv}_{\mathbf{Game}_6} - \Pr[\mathbf{F}']$

# Proof: Invalid ciphertexts

- **Game**$_7$: we abort (with a random output $b'$)
  in case of bad accepted ciphertext,
  we do as in **Game**$_1$

**Event $\mathbf{F}'$**

$\mathcal{A}$ submits a bad accepted ciphertext
(note: this is not computationally detectable)

The advantage in **Game**$_7$ is: $\Pr_{\mathbf{Game}_7}[b' = b | \mathbf{F}'] = 1/2$

$$\Pr_{\mathbf{Game}_6}[\mathbf{F}'] = \Pr_{\mathbf{Game}_7}[\mathbf{F}'] \qquad \Pr_{\mathbf{Game}_7}[b' = b | \neg\mathbf{F}'] = \Pr_{\mathbf{Game}_6}[b' = b | \neg\mathbf{F}']$$

$\Longrightarrow$ **Hop-S-Negl**: $\mathbf{Adv}_{\mathbf{Game}_7} \geq \mathbf{Adv}_{\mathbf{Game}_6} - \Pr[\mathbf{F}']$

## Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}']$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = {u_1}^{x_1+\alpha y_1} {u_2}^{x_2+\alpha y_2}$

Let us use "*" for all the elements related to the challenge ciphertext.

Three cases may appear:

- Case 1: $(u_1, u_2, e) = (u_1^*, u_2^*, e^*)$, then necessarily

$$v \neq v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = {u_1^*}^{x_1+\alpha^* y_1} {u_2^*}^{x_2+\alpha^* y_2}$$

  Then, the ciphertext is rejected $\Longrightarrow \Pr[\mathbf{F}'_1] = 0$
- Case 2: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$:
  From the previous game, Aborts $\Longrightarrow \Pr[\mathbf{F}'_2] = 0$
- Case 3: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, and $\alpha \neq \alpha^*$

## Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}']$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = {u_1}^{x_1+\alpha y_1} {u_2}^{x_2+\alpha y_2}$

Let us use "*" for all the elements related to the challenge ciphertext.

Three cases may appear:

- Case 1: $(u_1, u_2, e) = (u_1^*, u_2^*, e^*)$, then necessarily

$$v \neq v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = {u_1^*}^{x_1+\alpha^* y_1} {u_2^*}^{x_2+\alpha^* y_2}$$

  Then, the ciphertext is rejected $\implies \Pr[\mathbf{F}'_1] = 0$
- Case 2: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$:
  From the previous game, Aborts $\implies \Pr[\mathbf{F}'_2] = 0$
- Case 3: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, and $\alpha \neq \alpha^*$

# Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}']$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = {u_1}^{x_1+\alpha y_1} {u_2}^{x_2+\alpha y_2}$

Let us use "*" for all the elements related to the challenge ciphertext.

Three cases may appear:

- Case 1: $(u_1, u_2, e) = (u_1^*, u_2^*, e^*)$, then necessarily

$$v \neq v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = {u_1^*}^{x_1+\alpha^* y_1} {u_2^*}^{x_2+\alpha^* y_2}$$

  Then, the ciphertext is rejected $\Longrightarrow \Pr[\mathbf{F}'_1] = 0$
- Case 2: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$:
  From the previous game, Aborts $\Longrightarrow \Pr[\mathbf{F}'_2] = 0$
- Case 3: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, and $\alpha \neq \alpha^*$

In order to evaluate $\Pr[\mathbf{F}']$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = {u_1}^{x_1+\alpha y_1} {u_2}^{x_2+\alpha y_2}$

Let us use "*" for all the elements related to the challenge ciphertext.

Three cases may appear:

- Case 1: $(u_1, u_2, e) = (u_1^*, u_2^*, e^*)$, then necessarily

$$v \neq v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = {u_1^*}^{x_1+\alpha^* y_1} {u_2^*}^{x_2+\alpha^* y_2}$$

  Then, the ciphertext is rejected $\Longrightarrow \Pr[\mathbf{F}'_1] = 0$
- Case 2: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$:
  From the previous game, Aborts $\Longrightarrow \Pr[\mathbf{F}'_2] = 0$
- Case 3: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, and $\alpha \neq \alpha^*$

## Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}']$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = {u_1}^{x_1+\alpha y_1} {u_2}^{x_2+\alpha y_2}$

Let us use "*" for all the elements related to the challenge ciphertext.

Three cases may appear:

- Case 1: $(u_1, u_2, e) = (u_1^*, u_2^*, e^*)$, then necessarily

$$v \neq v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = {u_1^*}^{x_1+\alpha^* y_1} {u_2^*}^{x_2+\alpha^* y_2}$$

  Then, the ciphertext is rejected $\quad \Longrightarrow \Pr[\mathbf{F}'_1] = 0$
- Case 2: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$:
  From the previous game, Aborts $\quad \Longrightarrow \Pr[\mathbf{F}'_2] = 0$
- Case 3: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, and $\alpha \neq \alpha^*$

# Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}']$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = {u_1}^{x_1+\alpha y_1} {u_2}^{x_2+\alpha y_2}$

Let us use "*" for all the elements related to the challenge ciphertext.

Three cases may appear:

- Case 1: $(u_1, u_2, e) = (u_1^*, u_2^*, e^*)$, then necessarily

$$v \neq v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = {u_1^*}^{x_1+\alpha^* y_1} {u_2^*}^{x_2+\alpha^* y_2}$$

  Then, the ciphertext is rejected $\Longrightarrow \Pr[\mathbf{F}'_1] = 0$
- Case 2: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$:
  From the previous game, Aborts $\Longrightarrow \Pr[\mathbf{F}'_2] = 0$
- Case 3: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, and $\alpha \neq \alpha^*$

## Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}']$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = {u_1}^{x_1+\alpha y_1} {u_2}^{x_2+\alpha y_2}$

Let us use "*" for all the elements related to the challenge ciphertext.

Three cases may appear:

- Case 1: $(u_1, u_2, e) = (u_1^*, u_2^*, e^*)$, then necessarily

  $$v \neq v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = {u_1^*}^{x_1+\alpha^* y_1} {u_2^*}^{x_2+\alpha^* y_2}$$

  Then, the ciphertext is rejected $\implies \Pr[\mathbf{F}'_1] = 0$
- Case 2: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$:
  From the previous game, Aborts $\implies \Pr[\mathbf{F}'_2] = 0$
- Case 3: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, and $\alpha \neq \alpha^*$

# Details: Bad Accept

In order to evaluate $\Pr[\mathbf{F}']$, we study the probability that

- $r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$,
- whereas $v = {u_1}^{x_1+\alpha y_1} {u_2}^{x_2+\alpha y_2}$

Let us use "*" for all the elements related to the challenge ciphertext.

Three cases may appear:

- Case 1: $(u_1, u_2, e) = (u_1^*, u_2^*, e^*)$, then necessarily

$$v \neq v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = {u_1^*}^{x_1+\alpha^* y_1} {u_2^*}^{x_2+\alpha^* y_2}$$

  Then, the ciphertext is rejected $\implies \Pr[\mathbf{F}'_1] = 0$
- Case 2: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, but $\alpha = \alpha^*$:
  From the previous game, Aborts $\implies \Pr[\mathbf{F}'_2] = 0$
- Case 3: $(u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)$, and $\alpha \neq \alpha^*$

# Details: Bad Accept (Case 3)

The adversary knows the public key, and the (invalid) challenge ciphertext:

$$c = g_1^{x_1} g_2^{x_2} \qquad d = g_1^{y_1} g_2^{y_2}$$

$$v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = g_1^{r_1^*(x_1+\alpha^* y_1)} g_2^{r_2^*(x_2+\alpha^* y_2)}$$

Let us move to the exponents, in basis $g_1$, with $g_2 = g_1^s$:

$$\begin{aligned}
\log c &= x_1 + s x_2 \\
\log d &= y_1 + s y_2 \\
\log v^* &= r_1^*(x_1 + \alpha^* y_1) + s r_2^*(x_2 + \alpha^* y_2) \\
\log v &= r_1(x_1 + \alpha y_1) + s r_2(x_2 + \alpha y_2)
\end{aligned}$$

# Details: Bad Accept (Case 3)

The adversary knows the public key, and the (invalid) challenge ciphertext:

$$c = g_1^{x_1} g_2^{x_2} \qquad d = g_1^{y_1} g_2^{y_2}$$

$$v^* = U^{x_1+\alpha^* y_1} V^{x_2+\alpha^* y_2} = g_1^{r_1^*(x_1+\alpha^* y_1)} g_2^{r_2^*(x_2+\alpha^* y_2)}$$

Let us move to the exponents, in basis $g_1$, with $g_2 = g_1^s$:

$$\begin{aligned}
\log c &= x_1 + s x_2 \\
\log d &= y_1 + s y_2 \\
\log v^* &= r_1^*(x_1 + \alpha^* y_1) + s r_2^*(x_2 + \alpha^* y_2) \\
\log v &= r_1(x_1 + \alpha y_1) + s r_2(x_2 + \alpha y_2)
\end{aligned}$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\Delta = \begin{vmatrix} 1 & s & 0 & 0 \\ 0 & 0 & 1 & s \\ r_1^* & sr_2^* & r_1^*\alpha^* & sr_2^*\alpha^* \\ r_1 & sr_2 & r_1\alpha & sr_2\alpha \end{vmatrix}$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\begin{aligned}
\Delta &= \begin{vmatrix} 1 & s & 0 & 0 \\ 0 & 0 & 1 & s \\ r_1^* & sr_2^* & r_1^*\alpha^* & sr_2^*\alpha^* \\ r_1 & sr_2 & r_1\alpha & sr_2\alpha \end{vmatrix} \\
&= \begin{vmatrix} 0 & 1 & s \\ sr_2^* & r_1^*\alpha^* & sr_2^*\alpha^* \\ sr_2 & r_1\alpha & sr_2\alpha \end{vmatrix} - s \times \begin{vmatrix} 0 & 1 & s \\ r_1^* & r_1^*\alpha^* & sr_2^*\alpha^* \\ r_1 & r_1\alpha & sr_2\alpha \end{vmatrix}
\end{aligned}$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\Delta = \begin{vmatrix} 0 & 1 & s \\ sr_2^* & r_1^*\alpha^* & sr_2^*\alpha^* \\ sr_2 & r_1\alpha & sr_2\alpha \end{vmatrix} - s \times \begin{vmatrix} 0 & 1 & s \\ r_1^* & r_1^*\alpha^* & sr_2^*\alpha^* \\ r_1 & r_1\alpha & sr_2\alpha \end{vmatrix}$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\begin{aligned}
\Delta &= \begin{vmatrix} 0 & 1 & s \\ sr_2^* & r_1^*\alpha^* & sr_2^*\alpha^* \\ sr_2 & r_1\alpha & sr_2\alpha \end{vmatrix} - s \times \begin{vmatrix} 0 & 1 & s \\ r_1^* & r_1^*\alpha^* & sr_2^*\alpha^* \\ r_1 & r_1\alpha & sr_2\alpha \end{vmatrix} \\
&= s^2 \times \left( \begin{vmatrix} 0 & 1 & 1 \\ r_2^* & r_1^*\alpha^* & r_2^*\alpha^* \\ r_2 & r_1\alpha & r_2\alpha \end{vmatrix} - \begin{vmatrix} 0 & 1 & 1 \\ r_1^* & r_1^*\alpha^* & r_2^*\alpha^* \\ r_1 & r_1\alpha & r_2\alpha \end{vmatrix} \right)
\end{aligned}$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\Delta \quad = \quad s^2 \times \left( \begin{vmatrix} 0 & 1 & 1 \\ r_2^* & r_1^*\alpha^* & r_2^*\alpha^* \\ r_2 & r_1\alpha & r_2\alpha \end{vmatrix} - \begin{vmatrix} 0 & 1 & 1 \\ r_1^* & r_1^*\alpha^* & r_2^*\alpha^* \\ r_1 & r_1\alpha & r_2\alpha \end{vmatrix} \right)$$

The determinant of the system is

$$\begin{aligned}\Delta &= s^2 \times \left( \begin{vmatrix} 0 & 1 & 1 \\ r_2^* & r_1^*\alpha^* & r_2^*\alpha^* \\ r_2 & r_1\alpha & r_2\alpha \end{vmatrix} - \begin{vmatrix} 0 & 1 & 1 \\ r_1^* & r_1^*\alpha^* & r_2^*\alpha^* \\ r_1 & r_1\alpha & r_2\alpha \end{vmatrix} \right) \\ &= s^2 \times \left( \begin{array}{cc} r_2 \times \begin{vmatrix} 1 & 1 \\ r_1^*\alpha^* & r_2^*\alpha^* \end{vmatrix} & - \quad r_2^* \times \begin{vmatrix} 1 & 1 \\ r_1\alpha & r_2\alpha \end{vmatrix} \\ -r_1 \times \begin{vmatrix} 1 & 1 \\ r_1^*\alpha^* & r_2^*\alpha^* \end{vmatrix} & + \quad r_1^* \times \begin{vmatrix} 1 & 1 \\ r_1\alpha & r_2\alpha \end{vmatrix} \end{array} \right)\end{aligned}$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\Delta \quad = \quad s^2 \times \left( \begin{array}{cc} r_2 \times \begin{vmatrix} 1 & 1 \\ r_1^*\alpha^* & r_2^*\alpha^* \end{vmatrix} & - \quad r_2^* \times \begin{vmatrix} 1 & 1 \\ r_1\alpha & r_2\alpha \end{vmatrix} \\ -r_1 \times \begin{vmatrix} 1 & 1 \\ r_1^*\alpha^* & r_2^*\alpha^* \end{vmatrix} & + \quad r_1^* \times \begin{vmatrix} 1 & 1 \\ r_1\alpha & r_2\alpha \end{vmatrix} \end{array} \right)$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\Delta = s^2 \times \left( \begin{array}{ccc} r_2 \times \begin{vmatrix} 1 & 1 \\ r_1^*\alpha^* & r_2^*\alpha^* \end{vmatrix} & - & r_2^* \times \begin{vmatrix} 1 & 1 \\ r_1\alpha & r_2\alpha \end{vmatrix} \\ -r_1 \times \begin{vmatrix} 1 & 1 \\ r_1^*\alpha^* & r_2^*\alpha^* \end{vmatrix} & + & r_1^* \times \begin{vmatrix} 1 & 1 \\ r_1\alpha & r_2\alpha \end{vmatrix} \end{array} \right)$$

$$= s^2 \times \left( \begin{array}{ccc} r_2 \times (r_2^* - r_1^*) \times \alpha^* & - & r_2^* \times (r_2 - r_1) \times \alpha \\ -r_1 \times (r_2^* - r_1^*) \times \alpha^* & + & r_1^* \times (r_2 - r_1) \times \alpha \end{array} \right)$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\Delta = s^2 \times \left( \begin{array}{ccc} r_2 \times (r_2^* - r_1^*) \times \alpha^* & - & r_2^* \times (r_2 - r_1) \times \alpha \\ -r_1 \times (r_2^* - r_1^*) \times \alpha^* & + & r_1^* \times (r_2 - r_1) \times \alpha \end{array} \right)$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\begin{aligned}
\Delta &= s^2 \times \begin{pmatrix} r_2 \times (r_2^* - r_1^*) \times \alpha^* & - & r_2^* \times (r_2 - r_1) \times \alpha \\ -r_1 \times (r_2^* - r_1^*) \times \alpha^* & + & r_1^* \times (r_2 - r_1) \times \alpha \end{pmatrix} \\
&= s^2 \times ((r_2 - r_1) \times (r_2^* - r_1^*) \times \alpha^* - (r_2^* - r_1^*) \times (r_2 - r_1) \times \alpha)
\end{aligned}$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\Delta \quad = \quad s^2 \times ((r_2 - r_1) \times (r_2^* - r_1^*) \times \alpha^* - (r_2^* - r_1^*) \times (r_2 - r_1) \times \alpha)$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\begin{aligned}\Delta &= s^2 \times ((r_2 - r_1) \times (r_2^* - r_1^*) \times \alpha^* - (r_2^* - r_1^*) \times (r_2 - r_1) \times \alpha) \\ &= s^2 \times (r_2 - r_1) \times (r_2^* - r_1^*) \times (\alpha^* - \alpha)\end{aligned}$$

## Details: Bad Accept (Case 3)

The determinant of the system is

$$\Delta \quad = \quad s^2 \times (r_2 - r_1) \times (r_2^* - r_1^*) \times (\alpha^* - \alpha)$$

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\begin{aligned}\Delta &= s^2 \times (r_2 - r_1) \times (r_2^* - r_1^*) \times (\alpha^* - \alpha) \\ &\neq 0\end{aligned}$$

## Details: Bad Accept (Case 3)

The determinant of the system is

$$\begin{aligned}\Delta &= s^2 \times (r_2 - r_1) \times (r_2^* - r_1^*) \times (\alpha^* - \alpha) \\ &\neq 0\end{aligned}$$

The system is under-defined:
for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system

# Details: Bad Accept (Case 3)

The determinant of the system is

$$\begin{aligned} \Delta &= s^2 \times (r_2 - r_1) \times (r_2^* - r_1^*) \times (\alpha^* - \alpha) \\ &\neq 0 \end{aligned}$$

The system is under-defined:
for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system

$\Longrightarrow v$ is unpredictable

## Details: Bad Accept (Case 3)

The determinant of the system is

$$\begin{aligned}\Delta &= s^2 \times (r_2 - r_1) \times (r_2^* - r_1^*) \times (\alpha^* - \alpha) \\ &\neq 0\end{aligned}$$

The system is under-defined:
for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system

$\Longrightarrow$ $v$ is unpredictable $\qquad \Longrightarrow \Pr[\mathbf{F}_3'] \leq q_D/q$

## Details: Bad Accept (Case 3)

The determinant of the system is

$$\begin{array}{rcl} \Delta & = & s^2 \times (r_2 - r_1) \times (r_2^* - r_1^*) \times (\alpha^* - \alpha) \\ & \neq & 0 \end{array}$$

The system is under-defined:
for any $v$, there are $(x_1, x_2, y_1, y_2)$ that satisfy the system

$\implies v$ is unpredictable $\qquad \implies \Pr[\mathbf{F}'_3] \leq q_D/q$

$\implies \mathbf{Adv}_{\mathsf{Game}_7} \geq \mathbf{Adv}_{\mathsf{Game}_6} - q_D/q$

# Proof: Analysis of the Final Game

In the final **Game**$_7$:

- only valid ciphertexts are decrypted
- the challenge ciphertext contains

$$e = m_b \times U^{z_1} V^{z_2}$$

- the public key contains

$$h = g_1^{z_1} g_2^{z_2}$$

Again, the system is under-defined:
for any $m_b$, there are $(z_1, z_2)$ that satisfy the system
$\Longrightarrow m_b$ is unpredictable $\quad \Longrightarrow b$ is unpredictable
$\Longrightarrow \mathbf{Adv}_{\mathbf{Game}_7} = 0$

# Proof: Analysis of the Final Game

In the final **Game**$_7$:

- only valid ciphertexts are decrypted
- the challenge ciphertext contains
$$e = m_b \times U^{z_1} V^{z_2}$$
- the public key contains
$$h = g_1^{z_1} g_2^{z_2}$$

Again, the system is under-defined:
for any $m_b$, there are $(z_1, z_2)$ that satisfy the system
$\Longrightarrow m_b$ is unpredictable $\qquad \Longrightarrow b$ is unpredictable
$\Longrightarrow \mathbf{Adv}_{\mathbf{Game}_7} = 0$

## Proof: Analysis of the Final Game

In the final **Game**$_7$:

- only valid ciphertexts are decrypted
- the challenge ciphertext contains

$$e = m_b \times U^{z_1} V^{z_2}$$

- the public key contains

$$h = g_1^{z_1} g_2^{z_2}$$

Again, the system is under-defined:
for any $m_b$, there are $(z_1, z_2)$ that satisfy the system
$\Longrightarrow m_b$ is unpredictable $\quad \Longrightarrow b$ is unpredictable
$\Longrightarrow \mathbf{Adv}_{\mathbf{Game}_7} = 0$

# Proof: Analysis of the Final Game

In the final $\mathbf{Game}_7$:

- only valid ciphertexts are decrypted
- the challenge ciphertext contains

$$e = m_b \times U^{z_1} V^{z_2}$$

- the public key contains

$$h = g_1^{z_1} g_2^{z_2}$$

Again, the system is under-defined:
for any $m_b$, there are $(z_1, z_2)$ that satisfy the system
$\Longrightarrow m_b$ is unpredictable $\qquad \Longrightarrow b$ is unpredictable
$\Longrightarrow \mathbf{Adv}_{\mathbf{Game}_7} = 0$

# Proof: Analysis of the Final Game

In the final $\textbf{Game}_7$:

- only valid ciphertexts are decrypted
- the challenge ciphertext contains

$$e = m_b \times U^{z_1} V^{z_2}$$

- the public key contains

$$h = g_1^{z_1} g_2^{z_2}$$

Again, the system is under-defined:
for any $m_b$, there are $(z_1, z_2)$ that satisfy the system
$\Longrightarrow m_b$ is unpredictable $\quad \Longrightarrow b$ is unpredictable
$\Longrightarrow \mathbf{Adv}_{\textbf{Game}_7} = 0$

## Proof: Analysis of the Final Game

In the final **Game**$_7$:

- only valid ciphertexts are decrypted
- the challenge ciphertext contains
$$e = m_b \times U^{z_1} V^{z_2}$$
- the public key contains
$$h = g_1^{z_1} g_2^{z_2}$$

Again, the system is under-defined:
for any $m_b$, there are $(z_1, z_2)$ that satisfy the system
$\Longrightarrow m_b$ is unpredictable $\quad \Longrightarrow b$ is unpredictable
$\Longrightarrow \mathbf{Adv}_{\mathbf{Game}_7} = 0$

# Proof: Analysis of the Final Game

In the final $\mathbf{Game}_7$:

- only valid ciphertexts are decrypted
- the challenge ciphertext contains

$$e = m_b \times U^{z_1} V^{z_2}$$

- the public key contains

$$h = g_1^{z_1} g_2^{z_2}$$

Again, the system is under-defined:
for any $m_b$, there are $(z_1, z_2)$ that satisfy the system
$\Longrightarrow m_b$ is unpredictable $\Longrightarrow b$ is unpredictable
$\Longrightarrow \mathbf{Adv}_{\mathbf{Game}_7} = 0$

# Proof: Analysis of the Final Game

In the final **Game**$_7$:

- only valid ciphertexts are decrypted
- the challenge ciphertext contains
$$e = m_b \times U^{z_1} V^{z_2}$$
- the public key contains
$$h = g_1^{z_1} g_2^{z_2}$$

Again, the system is under-defined:
for any $m_b$, there are $(z_1, z_2)$ that satisfy the system
$\Longrightarrow m_b$ is unpredictable $\qquad \Longrightarrow b$ is unpredictable
$\Longrightarrow \mathbf{Adv}_{\mathsf{Game}_7} = 0$

# Conclusion

$$
\begin{array}{rcl}
\mathbf{Adv}_{\mathsf{Game}_7} & = & 0 \\
\mathbf{Adv}_{\mathsf{Game}_7} & \geq & \mathbf{Adv}_{\mathsf{Game}_6} - q_D/q \\
\mathbf{Adv}_{\mathsf{Game}_6} & \geq & \mathbf{Adv}_{\mathsf{Game}_5} - \mathbf{Succ}^{\mathcal{H}}(t) \\
\mathbf{Adv}_{\mathsf{Game}_5} & \geq & \mathbf{Adv}_{\mathsf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t) \\
\mathbf{Adv}_{\mathsf{Game}_4} & = & \mathbf{Adv}_{\mathsf{Game}_3} \\
\mathbf{Adv}_{\mathsf{Game}_3} & \geq & \mathbf{Adv}_{\mathsf{Game}_2} - q_D/q \\
\mathbf{Adv}_{\mathsf{Game}_2} & = & \mathbf{Adv}_{\mathsf{Game}_1} \\
\mathbf{Adv}_{\mathsf{Game}_1} & \geq & \mathbf{Adv}_{\mathsf{Game}_0} - q_D/q \\
\mathbf{Adv}_{\mathsf{Game}_0} & = & \mathbf{Adv}_{\mathcal{CS}}^{\mathsf{ind-cca}}(\mathcal{A})
\end{array}
$$

$$\mathbf{Adv}_{\mathcal{CS}}^{\mathsf{ind-cca}}(\mathcal{A}) \leq 2 \times \mathbf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t) + \mathbf{Succ}^{\mathcal{H}}(t) + 3q_D/q$$

# Conclusion

$$
\begin{aligned}
\mathbf{Adv}_{\textsf{Game}_7} &= 0 \\
\mathbf{Adv}_{\textsf{Game}_7} &\geq \mathbf{Adv}_{\textsf{Game}_6} - q_D/q \\
\mathbf{Adv}_{\textsf{Game}_6} &\geq \mathbf{Adv}_{\textsf{Game}_5} - \mathbf{Succ}^{\mathcal{H}}(t) \\
\mathbf{Adv}_{\textsf{Game}_5} &\geq \mathbf{Adv}_{\textsf{Game}_4} - 2 \times \mathbf{Adv}_{\mathbb{G}}^{\textsf{ddh}}(t) \\
\mathbf{Adv}_{\textsf{Game}_4} &= \mathbf{Adv}_{\textsf{Game}_3} \\
\mathbf{Adv}_{\textsf{Game}_3} &\geq \mathbf{Adv}_{\textsf{Game}_2} - q_D/q \\
\mathbf{Adv}_{\textsf{Game}_2} &= \mathbf{Adv}_{\textsf{Game}_1} \\
\mathbf{Adv}_{\textsf{Game}_1} &\geq \mathbf{Adv}_{\textsf{Game}_0} - q_D/q \\
\mathbf{Adv}_{\textsf{Game}_0} &= \mathbf{Adv}_{\mathcal{CS}}^{\textsf{ind}-\textsf{cca}}(\mathcal{A})
\end{aligned}
$$

$$
\mathbf{Adv}_{\mathcal{CS}}^{\textsf{ind}-\textsf{cca}}(\mathcal{A}) \leq 2 \times \mathbf{Adv}_{\mathbb{G}}^{\textsf{ddh}}(t) + \mathbf{Succ}^{\mathcal{H}}(t) + 3q_D/q
$$

# Outline

Basic Security Notions

Game-based Proofs

**Advanced Security for Encryption**

- Advanced Security Notions
- Cramer-Shoup Encryption Scheme
- Generic Conversion

Conclusion

# First Generic Conversion

[Bellare-Rogaway – Eurocrypt '93]

For efficiency: random oracle model

**Setup**

- A trapdoor one-way permutation family $\{(f, g)\}$ onto the set $X$
- Two hash functions, for the security parameter $k_1$,

$$\mathcal{G} : X \longrightarrow \{0,1\}^n \text{ and } \mathcal{H} : \{0,1\}^\star \longrightarrow \{0,1\}^{k_1},$$

where $n$ is the bit-length of the plaintexts.

**Key Generation**

One chooses a random element in the family

- $f$ is the public key
- the inverse $g$ is the private key

# First Generic Conversion

[Bellare-Rogaway – Eurocrypt '93]

For efficiency: random oracle model

## Setup

- A trapdoor one-way permutation family $\{(f, g)\}$ onto the set $X$
- Two hash functions, for the security parameter $k_1$,

$$\mathcal{G} : X \longrightarrow \{0,1\}^n \text{ and } \mathcal{H} : \{0,1\}^\star \longrightarrow \{0,1\}^{k_1},$$

  where $n$ is the bit-length of the plaintexts.

## Key Generation

One chooses a random element in the family

- $f$ is the public key
- the inverse $g$ is the private key

# First Generic Conversion (Cont'ed)

## Encryption

One chooses a random element $r \in X$

$$a = f(r), \quad b = m \oplus \mathcal{G}(r), \quad c = \mathcal{H}(m, r)$$

## Decryption

Given $(a, b, c)$, and the private key $g$,

- one first recovers $r = g(a)$
- one gets $m = b \oplus \mathcal{G}(r)$
- one then checks whether $c \stackrel{?}{=} \mathcal{H}(m, r)$

If the equality holds, one returns $m$,
otherwise one rejects the ciphertext

# First Generic Conversion (Cont'ed)

## Encryption

One chooses a random element $r \in X$

$$a = f(r), \quad b = m \oplus \mathcal{G}(r), \quad c = \mathcal{H}(m, r)$$

## Decryption

Given $(a, b, c)$, and the private key $g$,

- one first recovers $r = g(a)$
- one gets $m = b \oplus \mathcal{G}(r)$
- one then checks whether $c \stackrel{?}{=} \mathcal{H}(m, r)$

If the equality holds, one returns $m$,
otherwise one rejects the ciphertext

# Security of the Bellare-Rogaway Conversion

**Theorem**

*The Bellare-Rogaway conversion achieves* $\mathbf{IND-CCA}$ *security, under the one-wayness of the trapdoor permutation* $f$*:*

$$\mathbf{Adv}^{\mathsf{ind-cca}}_{\mathcal{BR}}(t) \leq 2 \times \mathbf{Succ}^{\mathsf{ow}}_{f}(T) + \frac{4q_D}{2^{k_1}},$$

*where* $T \leq t + (q_G + q_H) \cdot T_f$.

Let us prove this theorem, with a sequence of games, in which $\mathcal{A}$ is an $\mathbf{IND-CCA}$ adversary against the Bellare-Rogaway conversion.

# Security of the Bellare-Rogaway Conversion

**Theorem**

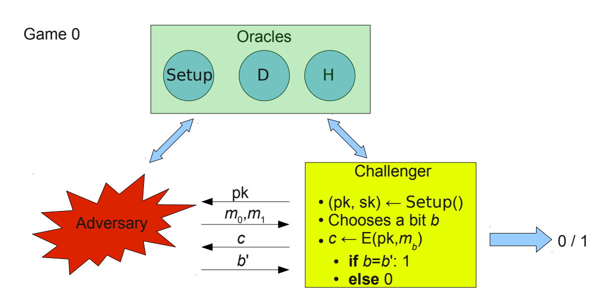
*The Bellare-Rogaway conversion achieves* $\mathbf{IND-CCA}$ *security, under the one-wayness of the trapdoor permutation* $f$*:*

$$\mathbf{Adv}^{\mathsf{ind-cca}}_{\mathcal{BR}}(t) \leq 2 \times \mathbf{Succ}^{\mathsf{ow}}_{f}(T) + \frac{4q_D}{2^{k_1}},$$

*where* $T \leq t + (q_G + q_H) \cdot T_f$*.*

Let us prove this theorem, with a sequence of games, in which $\mathcal{A}$ is an $\mathbf{IND-CCA}$ adversary against the Bellare-Rogaway conversion.

# Real Attack Game




## Key Generation Oracle

Random permutation $f$, and its inverse $g$

## Decryption Oracle

Compute $r = g(a)$, and then $m = b \oplus \mathcal{G}(r)$

if $c = \mathcal{H}(m, r)$, outputs $m$, otherwise reject

# Simulation of the Random Oracles

- **Game**$_0$: use of the perfect oracles

**Challenge Ciphertext**

Random $r$, random bit $b$: $a = f(r)$, $b = m_b \oplus \mathcal{G}(r)$, $c = \mathcal{H}(m, r)$

$$\mathbf{Adv}_{\textbf{Game}_0} = 2 \times \Pr_{\textbf{Game}_0}[b' = b] - 1 = \varepsilon$$

- **Game**$_1$: use of the simulation of the random oracles

**Random Oracles**

For any new query, a new random output: management of lists

$$\mathbf{Adv}_{\textbf{Game}_1} = \mathbf{Adv}_{\textbf{Game}_0}$$

# Simulation of the Random Oracles

- **$\textbf{Game}_0$**: use of the perfect oracles

**Challenge Ciphertext**

Random $r$, random bit $b$: $a = f(r)$, $b = m_b \oplus \mathcal{G}(r)$, $c = \mathcal{H}(m, r)$

$$\mathbf{Adv}_{\textbf{Game}_0} = 2 \times \Pr_{\textbf{Game}_0}[b' = b] - 1 = \varepsilon$$

- **$\textbf{Game}_1$**: use of the simulation of the random oracles

**Random Oracles**

For any new query, a new random output: management of lists

$$\mathbf{Adv}_{\textbf{Game}_1} = \mathbf{Adv}_{\textbf{Game}_0}$$

# Simulation of the Challenge Ciphertext

- **Game$_2$**: use of an independent random value $h^+$

**Challenge Ciphertext**

Random $r$, random bit $b$: $a = f(r)$, $b = m_b \oplus \mathcal{G}(r)$, $c = h^+$

This game is indistinguishable from the previous one, unless $(m_b, r)$ is queried to $\mathcal{H}$: event **AskMR** (it can only be asked by the adversary, since such a query by the decryption oracle would be for the challenge ciphertext).

Note that in case of **AskMR**, we stop the simulation with a random output:

$$\mathbf{Adv}_{\textbf{Game}_2} \geq \mathbf{Adv}_{\textbf{Game}_1} - 2 \times \Pr_{\textbf{Game}_2}[\textbf{AskMR}]$$

# Simulation of the Decryption Oracle

- **Game$_3$**: reject if $(m, r)$ not queried to $\mathcal{H}$

**Decryption Oracle**

Look in the $\mathcal{H}$-list for $(m, r)$ such that $c = \mathcal{H}(m, r)$.
If not found: reject,
if for one pair, $a = f(r)$ and $b = m \oplus \mathcal{G}(r)$, output $m$

This makes a difference if this value $c$, without having been asked to $\mathcal{H}$, is correct: for each attempt, the probability is bounded by $1/2^{k_1}$:

$$\begin{aligned} \mathbf{Adv}_{\textbf{Game}_3} &\geq \mathbf{Adv}_{\textbf{Game}_2} - 2q_D/2^{k_1} \\ \Pr_{\textbf{Game}_3}[\textbf{AskMR}] &\geq \Pr_{\textbf{Game}_2}[\textbf{AskMR}] - q_D/2^{k_1} \end{aligned}$$

# Simulation of the Challenge Ciphertext

- **Game$_4$**: use of an independent random value $g^+$ (and $h^+$)

**Challenge Ciphertext**

Random $r$, random bit $b$: $a = f(r)$, $b = m_b \oplus g^+$, $c = h^+$

This game is indistinguishable from the previous one, unless $r$ is queried to $\mathcal{G}$ by the adversary or by the decryption oracle. We denote by **AskR** the event that $r$ is asked to $\mathcal{G}$ or $\mathcal{H}$ by the adversary (which includes **AskMR**). But $r$ cannot be asked to $\mathcal{G}$ by the decryption oracle without **AskR**: only possible if $r$ is in the $\mathcal{H}$-list, and thus asked by the adversary:

$$\begin{aligned} \mathbf{Adv}_{\textbf{Game}_4} &\geq \mathbf{Adv}_{\textbf{Game}_3} - 2 \times \Pr_{\textbf{Game}_3}[\textbf{AskR} \wedge \neg\textbf{AskMR}] \\ \Pr_{\textbf{Game}_4}[\textbf{AskR}] &= \Pr_{\textbf{Game}_3}[\textbf{AskMR}] + \Pr_{\textbf{Game}_3}[\textbf{AskR} \wedge \neg\textbf{AskMR}] \end{aligned}$$

# Simulation of the Challenge Ciphertext

- **Game**$_5$: use of an independent random value $a^+$ (and $g^+$, $h^+$)

**Challenge Ciphertext**

random bit $b$: $a = a^+$, $b = m_b \oplus g^+$, $c = h^+$

This determines $r$, the unique value such that $a^+ = f(r)$, which allows to detect event **AskR.**

This game is perfectly indistinguishable from the previous one:

$$\begin{aligned} \mathbf{Adv}_{\textbf{Game}_5} &= \mathbf{Adv}_{\textbf{Game}_4} \\ \Pr_{\textbf{Game}_5}[\textbf{AskR}] &= \Pr_{\textbf{Game}_4}[\textbf{AskR}] \end{aligned}$$

# Inversion of the Permutation

Since we can assume that $a^+$ is a given challenge for inverting the permutation $f$, when one looks in the $\mathcal{G}$-list or the $\mathcal{H}$-list, one can find $r$, the pre-image of $a^+$:

$$\Pr_{\textbf{Game}_5}[\textbf{AskR}] \leq \mathbf{Succ}_f^{\mathsf{ow}}(t + (q_G + q_H) \cdot T_f)$$

But clearly, in the last game, because of $g^+$ that perfectly hides $m_b$:

$$\mathbf{Adv}_{\textbf{Game}_5} = 0$$

# Conclusion

As a consequence, $0 = \mathbf{Adv}_{\mathbf{Game}_5}$

$$\begin{aligned}
&= \mathbf{Adv}_{\mathbf{Game}_4} \geq \mathbf{Adv}_{\mathbf{Game}_3} - 2 \times \Pr_{\mathbf{Game}_3}[\mathbf{AskR} \wedge \neg\mathbf{AskMR}] \\
&\geq \mathbf{Adv}_{\mathbf{Game}_2} - 2 \times \Pr_{\mathbf{Game}_3}[\mathbf{AskR} \wedge \neg\mathbf{AskMR}] - 2q_D/2^{k_1} \\
&\geq \mathbf{Adv}_{\mathbf{Game}_1} - 2 \times \Pr_{\mathbf{Game}_2}[\mathbf{AskMR}] - 2 \times \Pr_{\mathbf{Game}_3}[\mathbf{AskR} \wedge \neg\mathbf{AskMR}] - 2q_D/2^{k_1} \\
&\geq \mathbf{Adv}_{\mathbf{Game}_0} - 2 \times \Pr_{\mathbf{Game}_3}[\mathbf{AskMR}] - 2 \times \Pr_{\mathbf{Game}_3}[\mathbf{AskR} \wedge \neg\mathbf{AskMR}] - 4q_D/2^{k_1} \\
&\geq \mathbf{Adv}_{\mathbf{Game}_0} - 2 \times \Pr_{\mathbf{Game}_4}[\mathbf{AskR}] - 4q_D/2^{k_1} \\
&\geq \mathbf{Adv}_{\mathbf{Game}_0} - 2 \times \Pr_{\mathbf{Game}_5}[\mathbf{AskR}] - 4q_D/2^{k_1}
\end{aligned}$$

And then,

$$\mathbf{Adv}_{\mathbf{Game}_0} \leq 4q_D/2^{k_1} + 2 \times \mathbf{Succ}_f^{\mathsf{ow}}(T)$$

# Conclusion

# Outline

# Conclusion

Game-based Methodology: the story of OAEP [Bellare-Rogaway EC '94]

# Conclusion

Game-based Methodology: the story of OAEP [Bellare-Rogaway EC '94]

- Reduction proven indistinguishable for an IND-CCA adversary (actually IND-CCA1, and not IND-CCA2) but widely believed for IND-CCA2, without any further analysis of the reduction
  **The direct-reduction methodology**
- [Shoup - Crypto '01]
  Shoup showed the gap for IND-CCA2, under the OWP
  **Granted his new game-based methodology**
- [Fujisaki-Okamoto-Pointcheval-Stern – Crypto '01]
  FOPS proved the security for IND-CCA2, under the PD-OWP
  **Using the game-based methodology**

# Conclusion

Game-based Methodology: the story of OAEP [Bellare-Rogaway EC '94]

- Reduction proven indistinguishable for an IND-CCA adversary (actually IND-CCA1, and not IND-CCA2) but widely believed for IND-CCA2, without any further analysis of the reduction
  **The direct-reduction methodology**
- [Shoup - Crypto '01]
  Shoup showed the gap for IND-CCA2, under the OWP
  **Granted his new game-based methodology**
- [Fujisaki-Okamoto-Pointcheval-Stern – Crypto '01]
  FOPS proved the security for IND-CCA2, under the PD-OWP
  **Using the game-based methodology**

# Conclusion

Game-based Methodology: the story of OAEP [Bellare-Rogaway EC '94]

- Reduction proven indistinguishable for an IND-CCA adversary (actually IND-CCA1, and not IND-CCA2) but widely believed for IND-CCA2, without any further analysis of the reduction
  **The direct-reduction methodology**
- [Shoup - Crypto '01]
  Shoup showed the gap for IND-CCA2, under the OWP
  **Granted his new game-based methodology**
- [Fujisaki-Okamoto-Pointcheval-Stern – Crypto '01]
  FOPS proved the security for IND-CCA2, under the PD-OWP
  **Using the game-based methodology**