Formal and Strong Security Definitions:

IND-CCA security

There are three kinds of lies:
small lies, big lies and statistics.

Sven Laur
swen@math.ut.ee

Helsinki University of Technology

Quick reminder

Semantic security

$m \leftarrow \mathcal{M}_0$

$$\xrightarrow{\mathsf{pk}, \mathcal{E}_{\mathsf{pk}}(m)}$$

Given
- pk
- $\mathcal{M}_0$
- $\mathcal{E}_{\mathsf{pk}}(m)$

Charlie tries to guess $g(m)$

$m \leftarrow \mathcal{M}_0$

Given
- $\mathcal{M}_0$

Charlie tries to guess $g(m)$

Homological classification

$$
\begin{tikzcd}
\text{NM-CPA} \arrow[d, Rightarrow] & \text{NM-CCA1} \arrow[l, Rightarrow] \arrow[d, Rightarrow] & \text{NM-CCA2} \arrow[l, Rightarrow] \arrow[d, Leftrightarrow] \\
\text{IND-CPA} & \text{IND-CCA1} \arrow[l, Rightarrow] & \text{IND-CCA2} \arrow[l, Rightarrow]
\end{tikzcd}
$$

The figure above depicts the relations among various security properties of public key cryptosystems. In practise one normally needs:

- ▷ semantic security that follows IND-CPA security,
- ▷ safety against improper usage that follows form IND-CCA1 security,
- ▷ non-malleability of ciphertexts that follows form NM-CPA security.

Homomorphic encryption

Formal definition

A cryptosystem $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ is homomorphic if for any $m_0, m_1 \leftarrow \mathcal{M}$

$$\mathcal{E}_{\mathsf{pk}}(m_0) \cdot \mathcal{E}_{\mathsf{pk}}(m_1) \equiv \mathcal{E}_{\mathsf{pk}}(m_0 \oplus m_1) \ \ .$$

The equivalence between distributions $\mathcal{E}_{\mathsf{pk}}(m_0) \cdot \mathcal{E}_{\mathsf{pk}}(m_1)$ and $\mathcal{E}_{\mathsf{pk}}(m_0 \oplus m_1)$ must hold even if we fix a single ciphertext $\mathcal{E}_{\mathsf{pk}}(m_0) = c$.

Homomorphic encryption facilitates limited crypto-computing:

- $\mathcal{D}_{\mathsf{sk}}(c_0 \cdot c_1) = \mathcal{D}_{\mathsf{sk}}(c_0) \oplus \mathcal{D}_{\mathsf{sk}}(c_1)$
- Assume that $0 \oplus m = m = m \oplus 0$. Then given a ciphertext $c \cdot \mathcal{E}_{\mathsf{pk}}(0)$, we can only restore $\mathcal{D}_{\mathsf{sk}}(c)$ even if we use infinite computing power.

Some homomorphic cryptosystems

The RSA cryptosystem is multiplicatively homomorphic over $\mathbb{Z}_N$

$$\mathcal{E}_{\mathsf{pk}}(m_0) \cdot \mathcal{E}_{\mathsf{pk}}(m_1) = {m_0}^e \cdot {m_1}^e = (m \cdot m_1)^e = \mathcal{E}_{\mathsf{pk}}(m_0 \cdot m_1)$$

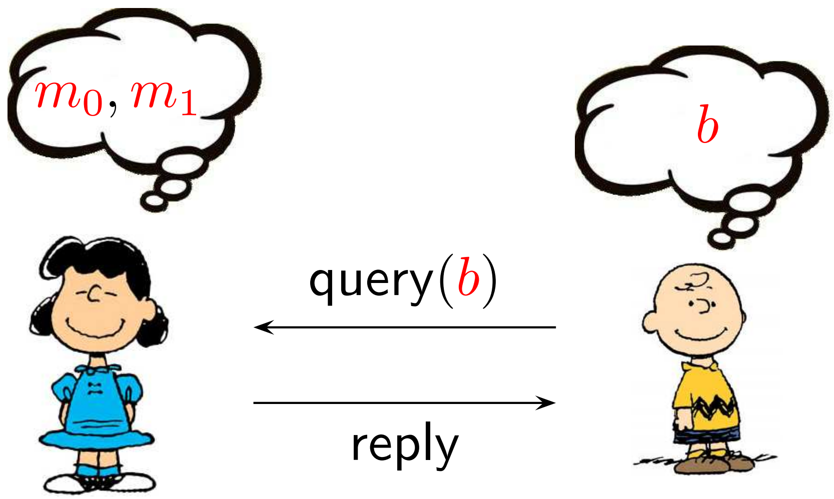
The Goldwasser-Micali cryptosystem is additively homomorphic over $\mathbb{Z}_2$

$$\mathcal{E}_{\mathsf{pk}}(m_0) \cdot \mathcal{E}_{\mathsf{pk}}(m_1) = x_0^2 \cdot y^{m_0} \cdot x_1^2 \cdot y^{m_1} \equiv x^2 \cdot y^{m_0 \oplus m_1} = \mathcal{E}_{\mathsf{pk}}(m_0 \oplus m_1) \ .$$

The ElGamal cryptosystem is multiplicatively homomorphic over G

$$\begin{aligned} \mathcal{E}_{\mathsf{pk}}(m_0) \cdot \mathcal{E}_{\mathsf{pk}}(m_1) &= (g^{k_0}, m_0 \cdot y^{k_0}) \cdot (g^{k_1}, m_1 \cdot y^{k_1}) \\ &= (g^{k_0+k_1}, m_0 \cdot m_1 \cdot y^{k_0+k_1}) \equiv \mathcal{E}_{\mathsf{pk}}(m_0 \cdot m_1) \ . \end{aligned}$$

Applications. Oblivious transfer



Alice should not distinguish
– query(0) and query(1)

Charlie should learn
– m_b and nothing more

One-out-of-two oblivious transfer protocol is particularly useful as it allows us to securely evaluate any function. Oblivious transfer can be used for

▷ authentication and access control,

▷ pay-per-view services and untraceable e-cash.

Homomorphic oblivious transfer

Assumptions

– Alice knows that Bob public key pk is well-formed.

– The cryptosystem is additively homomorphic and $|\mathcal{M}|$ is prime.

Protocol

1. Bob sends $\mathcal{E}_{\mathsf{pk}}(b)$ to Alice.
2. Alice computes $c_0 \leftarrow \mathcal{E}_{\mathsf{pk}}(b)^{r_0} \cdot \mathcal{E}_{\mathsf{pk}}(m_0)$ for $r_0 \leftarrow \mathcal{M}$.
3. Alice computes $c_1 \leftarrow (\mathcal{E}_{\mathsf{pk}}(b) \cdot \mathcal{E}_{\mathsf{pk}}(-1))^{r_1} \cdot \mathcal{E}_{\mathsf{pk}}(m_1)$ for $r_1 \leftarrow \mathcal{M}$.
4. Alice sends c_0, c_1 to Bob. Bob computes $m_b = \mathcal{D}_{\mathsf{sk}}(c_b)$.

Note that

$$c_0 = \mathcal{E}_{\mathsf{pk}}(br_0 + m_0) \qquad \text{and} \qquad c_1 = \mathcal{E}_{\mathsf{pk}}((b-1)r_1 + m_1) \ .$$

Security of oblivious transfer

If the cryptosystem is IND-CPA secure then Alice learns nothing about b.

Bob can learn only one of the messages m_0 or m_1, since

- if $b \neq 0$ then br_0 is uniformly distributed over $\mathcal{M}$,
- if $b \neq 1$ then $(b-1)r_1$ is uniformly distributed over $\mathcal{M}$.

Consequently

- if $b \neq 0$ then $\mathcal{D}_{\mathsf{sk}}(c_0)$ is uniformly distributed over $\mathcal{M}$,
- if $b \neq 1$ then $\mathcal{D}_{\mathsf{sk}}(c_1)$ is uniformly distributed over $\mathcal{M}$.

The latter is sufficient for security since even a unbounded adversary cannot learn anything beyond $\mathcal{D}_{\mathsf{sk}}(c_0)$ and $\mathcal{D}_{\mathsf{sk}}(c_1)$.

Is Bob guaranteed to know his input b?

What happens if Alice is malicious?

Example instantiations

Since the Goldwasser-Micali cryptosystem is IND-CPA secure and additively homomorphic over $\mathbb{Z}_2$. Then the implementation is straightforward.

We can make the ElGamal cryptosystem additively homomorphic by defining

$$\overline{\mathcal{E}}_{\mathsf{pk}}(m) = (g^k, g^m \cdot y^k)$$

as

$$\begin{aligned}\overline{\mathcal{E}}_{\mathsf{pk}}(m_0) \cdot \overline{\mathcal{E}}_{\mathsf{pk}}(m_1) &= (g^{k_0}, g^{m_0} \cdot y^{k_0}) \cdot (g^{k_1}, g^{m_1} \cdot y^{k_1}) \\ &= (g^{k_0+k_1}, g^{m_0+m_1} \cdot y^{k_0+k_1}) \equiv \overline{\mathcal{E}}_{\mathsf{pk}}(m_0 \cdot m_1) \enspace .\end{aligned}$$

Modified protocol

1. Bob sends $\overline{\mathcal{E}}_{\mathsf{pk}}(b) = (g^k, g^b \cdot y^k)$ to Alice.
2. Alice computes $c_0 \leftarrow \overline{\mathcal{E}}_{\mathsf{pk}}(b)^{r_0} \cdot \mathcal{E}_{\mathsf{pk}}(m_0)$ for $r_0 \leftarrow \mathcal{M}$, that is,

$$c_0 \leftarrow (g^k, g^b \cdot y^k)^{r_0} \cdot (g^{s_0}, m_0 \cdot y^{s_0}) = (g^{kr_0+s_0}, m_0 \cdot g^{br_0} \cdot y^{kr_0+s_0})$$

3. Alice computes $c_1 \leftarrow (\overline{\mathcal{E}}_{\mathsf{pk}}(b) \cdot \overline{\mathcal{E}}_{\mathsf{pk}}(-1))^{r_1} \cdot \mathcal{E}_{\mathsf{pk}}(m_1)$ for $r_1 \leftarrow \mathcal{M}$, that is,

$$\begin{aligned} c_1 &\leftarrow (g^{k-t}, g^{b-1} \cdot y^{k-t})^{r_1} \cdot (g^{s_1}, m_1 \cdot y^{s_1}) \\ &= (g^{(k-t)r_1+s_1}, m_1 \cdot g^{(b-1)r_1} \cdot y^{(k-t)r_1+s_1}) \end{aligned}$$

4. Alice sends c_0, c_1 to Bob. Bob computes $m_b = \mathcal{D}_{\mathsf{sk}}(c_b)$.

Applications. Blind signatures

Assume that Alice provides a public decryption service:

▷ Given a ciphertext c replies back the corresponding message $m = \mathcal{D}_{\mathsf{sk}}(c)$.

If the cryptosystem is multiplicatively homomorphic then Bob can decrypt the ciphertext c without revealing the corresponding message to Alice.

1. Bob computes $\overline{c} \leftarrow c \cdot \mathcal{E}_{\mathsf{pk}}(m_1)$ for $m_1 \leftarrow \mathcal{M}$.
2. Bob sends $\overline{c}$ to Alice. Alice replies $\overline{m} \leftarrow \mathcal{D}_{\mathsf{sk}}(\overline{c})$.
3. Bob restores the original message $m = \overline{m} \cdot m_1^{-1}$.

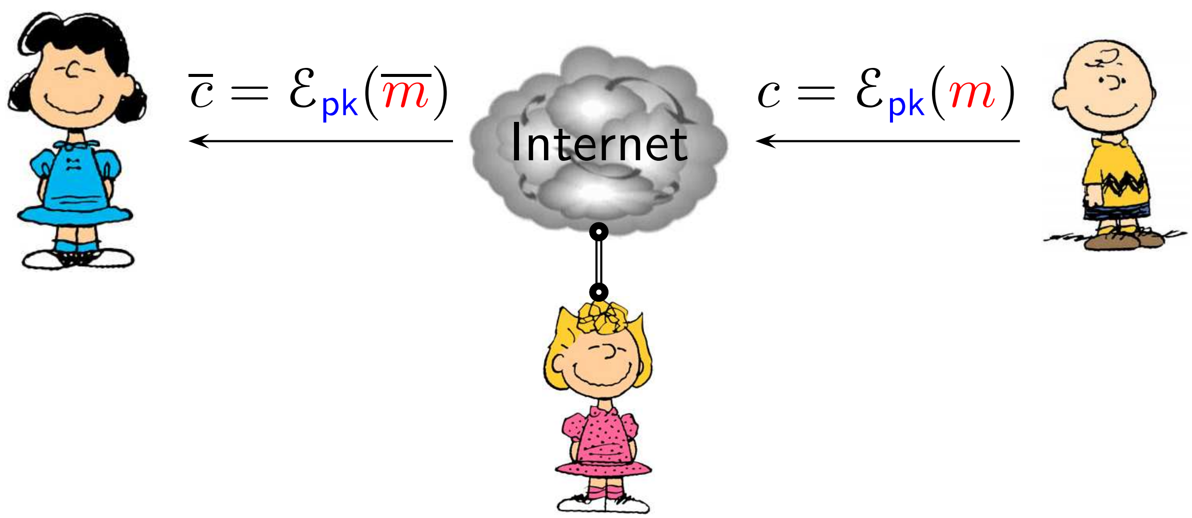
Recall that computing RSA signatures is just a decryption operation.

$\Rightarrow$ We get a protocol, where Alice can blindly sign documents.

$\Rightarrow$ Such signatures show that Alice still trusts Bob.

Ciphertext modification attacks

Active attack model



A malicious participant may control the communication network and alter the ciphertexts to bypass various security checks.

A non-malleable encryption has a specific detection mechanism that allows to detect modified ciphertexts or assures that m and $\overline{m}$ are unrelated.

Safety against improper usage

Cleverly crafted ciphertexts or ciphertext-like messages may provide relevant information about the secret key or even reveal the secret key.

Such attack naturally occur in:

- ▷ smart card cracking (Satellite TV, TPM-modules, ID cards)
- ▷ authentication protocols (challenge-response protocols)
- ▷ side channel attack (timing information, encryption failures)

Minimal security level:

- ▷ Attacks reveal information only about currently known ciphertexts

Affected cryptosystems:

– Rabin cryptosystem, some versions of NTRU cryptosystem, etc.

IND-CCA1 security

Malice is good in breaking security of a cryptosystem $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ if Malice can distinguish two games (interactive hypothesis testing):

Game $\mathcal{G}_0$	Game $\mathcal{G}_1$
1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{G}$	1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{G}$
2. $(m_0, m_1, \sigma) \leftarrow \mathsf{Malice}^{\mathcal{O}_1(\cdot)}(\mathsf{pk})$	2. $(m_0, m_1, \sigma) \leftarrow \mathsf{Malice}^{\mathcal{O}_1(\cdot)}(\mathsf{pk})$
3. $\mathsf{guess} \leftarrow \mathsf{Malice}(\sigma, \mathcal{E}_{\mathsf{pk}}(m_0))$	3. $\mathsf{guess} \leftarrow \mathsf{Malice}(\sigma, \mathcal{E}_{\mathsf{pk}}(m_1))$

with a *non-negligible* advantage*

$$\mathsf{Adv}(\mathsf{Malice}) = \left|\Pr\left[\mathsf{guess} = 0 | \mathcal{G}_0\right] - \Pr\left[\mathsf{guess} = 0 | \mathcal{G}_1\right]\right|$$

where the oracle $\mathcal{O}_1$ serves decryption queries, i.e., $\mathcal{O}_1(c) = \mathcal{D}_{\mathsf{sk}}(c)$.

*Twice larger than defined in the Mao's book

Rabin cryptosystem

Key generation $\mathcal{G}$:

1. Choose uniformly 512-bit prime numbers p and q.
2. Compute $N = p \cdot q$ and $\phi(N) = (p-1)(q-1)$.
3. Choose uniformly $e \leftarrow \mathbb{Z}^*_{\phi(N)}$ and set $d = e^{-1} \mod \phi(N)$.
4. Output sk $= (p, q, e, d)$ and pk $= (N, e)$.

Encryption and decryption:

$$\mathcal{M} = \mathbb{Z}_N, \quad \mathcal{C} = \mathbb{Z}_N, \quad \mathcal{R} = \emptyset$$

$$\mathcal{E}_{\mathsf{pk}}(m) = m^2 \mod N \qquad \mathcal{D}_{\mathsf{sk}}(c) = \sqrt{c} \mod N \ .$$

Lunchtime attack

1. Choose $x \leftarrow \mathbb{Z}_N$ and set $c \leftarrow m^2 \mod N$.
2. Compute decryption $\overline{x} \leftarrow \mathcal{O}_1(c)$.
3. If $\overline{x} \neq \pm x$ then
   - Compute nontrivial square root $\xi = \overline{x} \cdot x^{-1} \mod N$
   - Compute a nontrivial factors $p \leftarrow \gcd(N, \xi + 1)$ and $q = N/p$.
   - Output a secret key sk $= (p, q)$.
4. Continue from Step 1.

Efficiency analysis

- Each iteration succeeds with probability $\frac{1}{4}$.
- With 40 decryption queries the failure probability is 2^{-80}.

IND-CCA2 security

Malice is good in breaking security of a cryptosystem $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ if Malice can distinguish two games (interactive hypothesis testing):

Game $\mathcal{G}_0$	Game $\mathcal{G}_1$
1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{G}$	1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{G}$
2. $(m_0, m_1, \sigma) \leftarrow \mathsf{Malice}^{\mathcal{O}_1(\cdot)}(\mathsf{pk})$	2. $(m_0, m_1, \sigma) \leftarrow \mathsf{Malice}^{\mathcal{O}_1(\cdot)}(\mathsf{pk})$
3. $\mathsf{guess} \leftarrow \mathsf{Malice}^{\mathcal{O}_2(\cdot)}(\sigma, \mathcal{E}_{\mathsf{pk}}(m_0))$	3. $\mathsf{guess} \leftarrow \mathsf{Malice}^{\mathcal{O}_2(\cdot)}(\sigma, \mathcal{E}_{\mathsf{pk}}(m_1))$

with a *non-negligible* advantage*

$$\mathsf{Adv}(\mathsf{Malice}) = \left|\Pr\left[\mathsf{guess} = 0 | \mathcal{G}_0\right] - \Pr\left[\mathsf{guess} = 0 | \mathcal{G}_1\right]\right|$$

where the oracles $\mathcal{O}_1$ and $\mathcal{O}_2$ serve decryption queries, i.e., $\mathcal{O}_1(c) = \mathcal{D}_{\mathsf{sk}}(c)$ and $\mathcal{O}_2(c) = \mathcal{D}_{\mathsf{sk}}(c)$ for all non-challenge ciphertexts.

*Twice larger than defined in the Mao's book

IND-CCA2 secure cryptosystems

All known IND-CCA2 secure cryptosystems include a non-interactive proof that the creator of the ciphertexts c knows the corresponding message m:

- the RSA-OAEP cryptosystem in the random oracle model,
- the Cramer-Shoup cryptosystem in standard model,
- the Kurosawa-Desmedt key encapsulation scheme.

NM-CPA security

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

$\xrightarrow{\mathsf{pk}}$

$\xleftarrow{m_0, m_1}$

$\xrightarrow{\mathcal{E}_{\mathsf{pk}}(m_b)}$

$\xleftarrow{\hat{c}_1, \ldots, \hat{c}_n, \pi(\cdot)}$

Given $\mathcal{E}_{\mathsf{pk}}(m_b)$

Charlie tries to create

- ciphertexts $\hat{c}_1, \ldots, \hat{c}_n$
- a predicate $\pi(\cdot)$

such that

Output $\pi(m_b, \mathcal{D}_{\mathsf{sk}}(\hat{c}_1), \ldots, \mathcal{D}_{\mathsf{sk}}(\hat{c}_n))$

$\pi(m_b, \mathcal{D}_{\mathsf{sk}}(\hat{c}_1), \ldots, \mathcal{D}_{\mathsf{sk}}(\hat{c}_n)) = 1$

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

$\overline{b} \leftarrow \{0,1\}$

$\xrightarrow{\mathsf{pk}}$

$\xleftarrow{m_0, m_1}$

$\xrightarrow{\mathcal{E}_{\mathsf{pk}}(m_{\overline{b}})}$

$\xleftarrow{\hat{c}_1, \ldots, \hat{c}_n, \pi(\cdot)}$

Alice fools Chalie

Still Charlie tries to create

- ciphertexts $\hat{c}_1, \ldots, \hat{c}_n$
- a predicate $\pi(\cdot)$

such that

Output $\pi(m_b, \mathcal{D}_{\mathsf{sk}}(\hat{c}_1), \ldots, \mathcal{D}_{\mathsf{sk}}(\hat{c}_n))$

$\pi(m_b, \mathcal{D}_{\mathsf{sk}}(\hat{c}_1), \ldots, \mathcal{D}_{\mathsf{sk}}(\hat{c}_n)) = 1$

NM-CPA security

Charlie is good in breaking security of a cryptosystem $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ if Charlie can distinguish two games (interactive hypothesis testing) described in the precious slide with a *non-negligible* advantage*

$$\mathsf{Adv}(\mathsf{Malice}) = \left|\Pr\left[\mathsf{Alice} = 1|\mathcal{G}_0\right] - \Pr\left[\mathsf{Alice} = 1|\mathcal{G}_1\right]\right| \ ,$$

where Alice always outputs 0 is $c \in \{\hat{c}_1, \ldots, \hat{c}_n\}$ to eliminate cheating.

The game $\mathcal{G}_1$ can be simulated to Charlie without contacting Alice at all.

In other words, the Charlie's response vector $\hat{c}_1, \ldots, \hat{c}_n$ is computationally independent from the challenge ciphertext.

Homological classification

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

Horizontal implications are trivial.

- The adversary just gets more powerful in the row.

Downwards implications are trivial.

- A guess guess can be passed as relation $\rho(\cdot) \equiv 0$ and $\rho(\cdot) \equiv 1$.

IND-CCA2 security implies NM-CC2 security

Assume that Charlie is good in the NM-CCA2 game. Then we can emulate NM-CCA2 game given access to the oracle $\mathcal{O}_2$. Consider Malice:

1. Malice forwards pk to Charlie.
2. Malice forwards $m_{0\oplus b}, m_{1\oplus b}$ to Challenger for $b \leftarrow \{0,1\}$.
3. Malice forwards the challenge c to Charlie.
4. Charlie outputs $\hat{c}_1, \ldots, \hat{c}_n$ and $\pi(\cdot)$ to Malice who
   - uses $\mathcal{O}_2$ to recover $\mathcal{D}_{\mathsf{sk}}(\hat{c}_1), \ldots, \mathcal{D}_{\mathsf{sk}}(\hat{c}_n)$,
   - outputs $\pi(m_b, \mathcal{D}_{\mathsf{sk}}(\hat{c}_1), \ldots, \mathcal{D}_{\mathsf{sk}}(\hat{c}_n))$ as guess.

Running time

If $\pi(\cdot)$ is efficiently computable then Malice and Charlie have comparable running times.

How well does Malice perform?

In both game Malice outputs 1 only if $\pi(m_b, \mathcal{D}_{\mathsf{sk}}(\hat{c}_1), \ldots, \mathcal{D}_{\mathsf{sk}}(\hat{c}_n)) = 1$ and Charlie follows the rules of NM-CCA2 game. If Charlie follows the rules of NM-CCA2 game then Malice follows the rules of IND-CCA2 game. Now

$$\Pr\left[\mathsf{Malice} = 1 | \mathcal{G}_0\right] = \Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_0^{\mathsf{NM\text{-}CCA2}}\right] \quad ,$$

$$\Pr\left[\mathsf{Malice} = 1 | \mathcal{G}_1\right] = \Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_1^{\mathsf{NM\text{-}CCA2}}, b \neq \overline{b}\,\right] \quad .$$

As

$$\Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_0^{\mathsf{NM\text{-}CCA2}}\right] = \Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_1^{\mathsf{NM\text{-}CCA2}}, b = \overline{b}\,\right]$$

we obtain...

How well does Malice perform?

$$\Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_0^{\mathsf{NM\text{-}CCA2}}\right] = \frac{2}{2} \cdot \Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_1^{\mathsf{NM\text{-}CCA2}}, b = \overline{b}\right]$$

$$\Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_1^{\mathsf{NM\text{-}CCA2}}\right] = \frac{1}{2} \cdot \Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_1^{\mathsf{NM\text{-}CCA2}}, b = \overline{b}\right] + \frac{1}{2} \cdot \Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_1^{\mathsf{NM\text{-}CCA2}}, b \neq \overline{b}\right]$$

Thus

$$\begin{aligned}\mathsf{Adv}^{\mathsf{NM\text{-}CCA2}}(\mathsf{Charlie}) &= \frac{1}{2} \cdot \left|\Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_1^{\mathsf{NM\text{-}CCA2}}, b = \overline{b}\right] - \Pr\left[\mathsf{Alice} = 1 | \mathcal{G}_1^{\mathsf{NM\text{-}CCA2}}, b \neq \overline{b}\right]\right| \\ &= \frac{1}{2} \cdot \left|\Pr\left[\mathsf{Malice} = 1 | \mathcal{G}_0\right] - \Pr\left[\mathsf{Malice} = 1 | \mathcal{G}_1\right]\right| = \mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}(\mathsf{Malice}) \ .\end{aligned}$$

That is

$$\mathsf{Adv}^{\mathsf{NM\text{-}CCA1}}(\mathsf{Charlie}) = \frac{1}{2} \cdot \mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}(\mathsf{Malice}) \ .$$