Plaintext Awareness, Non-Malleability and Chosen Ciphertext Security: Implications and Separations

Mihir Bellare*, Anand Desai*, David Pointcheval† and Phillip Rogaway‡

* University of California at San Diego
† Université de Caen/École Normale Supérieure
‡ University of California at Davis

Summary

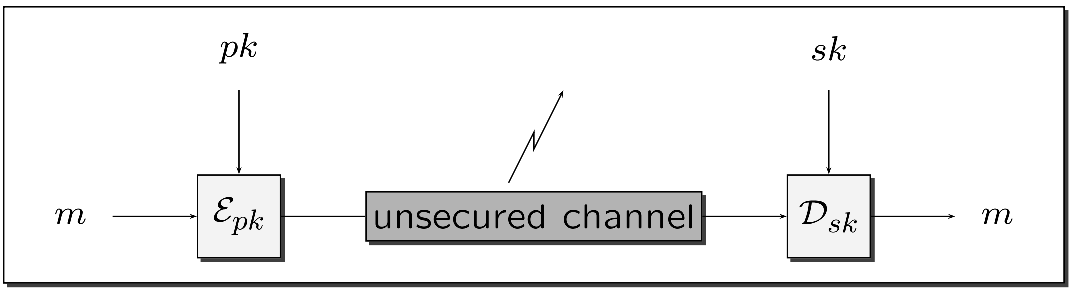
Introduction

- Encryption = Confidentiality = Security
  $\Longrightarrow$ many notions of security:
  from semantic security to plaintext awareness.
- The hierarchy is not well known
- Many schemes have been proposed and proven
  - in the standard model
  - in the random oracle model

Goal: clean-up this area

Encryption Schemes: definition

Public Key Encryption: confidentiality



$\mathcal{K}$	(Key Generation)	:	Security-Param $\rightarrow$ Public-Key $\times$ Secret-Key
$\mathcal{E}$	(Encryption)	:	Public-Key $\times$ Message $\rightarrow$ Ciphertext
$\mathcal{D}$	(Decryption)	:	Secret-Key $\times$ Ciphertext $\rightarrow$ Message $\cup \{*\}$

Encryption Schemes: notions of security

Perfect Security:
the ciphertext does not reveal anything
about the plaintext (except the size)

But this perfect security **is not** possible.
(except one-time pad)

Computational version: **Polynomial Security**
(Goldwasser–Micali 84)

a.k.a. Indistinguishability $\Longleftrightarrow$ *Semantic Security*.

PA, NM and CCS: Implications and Separations

Indistinguishability − *IND*

Encryption scheme: $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
Adversary: $A = (A_1, A_2)$

For any $k \in \mathsf{N}$ define $\mathsf{Adv}^{\mathsf{ind}}_{A,\Pi}(k) \stackrel{\mathsf{def}}{=}$

$$2 \cdot \Pr\left[(pk, sk) \leftarrow \mathcal{K}(1^k) \; ; \; (x_0, x_1, s) \leftarrow A_1(pk) \; ; \; b \leftarrow \{0,1\} \; ; \; y \leftarrow \mathcal{E}_{pk}(x_b) : \; A_2(x_0, x_1, s, y) = b\right] - 1 \; .$$

Π is *IND*-secure iff

A PPTM $\Longrightarrow \mathsf{Adv}^{\mathsf{ind}}_{A,\Pi}(k)$ negligible.

Chosen Ciphertext Security v1 – *CCS-1*

(Naor–Yung 1990)
a.k.a. lunchtime attack.

Encryption scheme: $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
Adversary: $A = (A_1, A_2)$

For any $k \in \mathrm{N}$ define $\mathrm{Adv}_{A,\Pi}^{\text{ccs-1}}(k) \stackrel{\text{def}}{=}$

$$2 \cdot \Pr\left[(pk, sk) \leftarrow \mathcal{K}(1^k) \; ; \; (x_0, x_1, s) \leftarrow A_1^{\mathcal{D}_{sk}}(pk) \; ; \; b \leftarrow \{0,1\} \; ; \; y \leftarrow \mathcal{E}_{pk}(x_b) : \; A_2(x_0, x_1, s, y) = b\right] - 1 \, .$$

Π is *CCS-1*-secure iff

A PPTM $\Longrightarrow \mathrm{Adv}_{A,\Pi}^{\text{ccs-1}}(k)$ negligible.

Chosen Ciphertext Security v2 – *CCS-2*

(Rackoff–Simon 1991)

Encryption scheme: $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
Adversary: $A = (A_1, A_2)$

For any $k \in \mathrm{N}$ define $\mathrm{Adv}_{A,\Pi}^{\text{ccs-2}}(k) \stackrel{\text{def}}{=}$

$$2 \cdot \Pr\left[(pk, sk) \leftarrow \mathcal{K}(1^k) \; ; \; (x_0, x_1, s) \leftarrow A_1^{\mathcal{D}_{sk}}(pk) \; ; \; b \leftarrow \{0,1\} \; ; \; y \leftarrow \mathcal{E}_{pk}(x_b) : \; A_2^{\mathcal{D}_{sk}}(x_0, x_1, s, y) = b\right] - 1 \, .$$

Π is *CCS-2*-secure iff

A PPTM $\Longrightarrow \mathrm{Adv}_{A,\Pi}^{\text{ccs-2}}(k)$ negligible.

Non-Malleability – NM

(Dolev–Dwork–Naor 1991)

Encryption scheme: $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
Adversary: $A = (A_1, A_2)$
Simulator: A_2^*

For any $k \in \mathsf{N}$: $\mathsf{Adv}^{\mathsf{nm}}_{A,A_2^*,\Pi}(k) \stackrel{\mathsf{def}}{=} \mathsf{Succ}^{\mathsf{nm}}_{A,\Pi}(k) - \mathsf{Succ}^{\mathsf{nm}}_{(A_1,A_2^*),\Pi}(k)$, where

$$\begin{aligned}\mathsf{Succ}^{\mathsf{nm}}_{A,\Pi}(k) &= \Pr[(pk, sk) \leftarrow \mathcal{K}(1^k)\ ;\ (M, R, s) \leftarrow A_1(pk)\ ;\ x \leftarrow M\ ; \\ &\qquad \alpha \leftarrow \mathcal{E}_{pk}(x)\ ;\ \alpha' \leftarrow A_2(\alpha, M, R, s) :\ R(x, \mathcal{D}_{sk}(\alpha'))] \\ \mathsf{Succ}^{\mathsf{nm}}_{(A_1,A_2^*),\Pi}(k) &= \Pr[(pk, sk) \leftarrow \mathcal{K}(1^k)\ ;\ (M, R, s) \leftarrow A_1(pk)\ ;\ x \leftarrow M\ ; \\ &\qquad \alpha' \leftarrow A_2^*(|x|, M, R, s, pk) :\ R(x, \mathcal{D}_{sk}(\alpha'))]\ .\end{aligned}$$

Π is NM iff

$\forall A$ PPTM $\exists A_2^*$ PPTM s.t. $\mathsf{Adv}^{\mathsf{nm}}_{A,A_2^*\Pi}(k)$ negligible.

Plaintext Awareness – PA

(Bellare–Rogaway 1994)

Encryption scheme: $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
Adversary: B
Knowledge extractor: K

For any $k \in \mathsf{N}$ define $\mathsf{Succ}^{\mathsf{pa}}_{K,B,\Pi}(k)$

$$\Pr[H \leftarrow \mathsf{Hash}\ ;\ (pk, sk) \leftarrow \mathcal{K}(1^k)\ ;\ (\mathit{Hlist}, \mathcal{E}\mathit{list}, y) \leftarrow \mathsf{run}\ B^{H,\mathcal{E}^H_{pk}}(pk) : \\ K(\mathit{Hlist}, \mathcal{E}\mathit{list}, y, pk) = \mathcal{D}^H_{sk}(y)\ \&\ y \notin \mathcal{E}\mathit{list}\ ]\ .$$

K is a $\lambda(k)$-extractor $\Longleftrightarrow \forall B$, $\mathsf{Succ}^{\mathsf{pa}}_{K,B,\Pi}(k) \geq \lambda(k)$.

Π is PA iff Π is IND-secure
and $\exists \lambda(k)$-extractor with $1 - \lambda(k)$ negligible

State of the Art

- **Semantic Security** (basic requirement for encryption schemes) is equivalent to Indistinguishability
- Many people are aware that $CCS\text{-}2 \Longrightarrow NM$ (no proof has never appeared)
- Bellare and Rogaway (Eurocrypt '94) hinted that $PA \Longrightarrow CCS\text{-}2$ (and NM).

Is it true? What about the other direction?
What about $CCS\text{-}1$ and NM?

Goals

Provide the confirmation of everything is assumed and study the relation between each possible pairs:

- Implication: proof
- Separation: counter-example

We would like everything to be true
independently of the model
(standard model, random oracle model, . . .)

Our relations

Proof of theorem 1: $\mathit{CCS}\text{-}\mathit{2} \Longrightarrow \mathit{NM}$

$\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is $\mathit{CCS}\text{-}\mathit{2}$-secure, is it NM-secure?

Let $A = (A_1, A_2)$ be an NM-adversary against Π,
we want to construct a simulator A_2^*:

$A_2^*(n, M, R, s, pk)$
  $x \leftarrow M$; $\alpha \leftarrow \mathcal{E}_{pk}(x)$
  $\alpha' \leftarrow A_2(\alpha, M, R, s)$
  Return α'

$\mathsf{Adv}^{\mathsf{nm}}_{A,A_2^*,\Pi}(k)$?

Proof (cont'd)

Let us consider the following *CCS-2*-attacker $B = (B_1, B_2)$:

$B_1^{\mathcal{D}_{sk}}(pk)$	$B_2^{\mathcal{D}_{sk}}(x_0, x_1, s' = (M, R, s), y = \mathcal{E}_{pk}(x_b))$
$(M, R, s) \leftarrow A_1(pk)$	$\alpha' \leftarrow A_2(y, M, R, s)$
$x_0 \leftarrow M$; $x_1 \leftarrow M$	if $R(x_0, \mathcal{D}_{sk}(\alpha'))$ then $d \leftarrow 0$
$s' \leftarrow (M, R, s)$	else $d \leftarrow \{0, 1\}$
Return (x_0, x_1, s')	Return d

$$\begin{aligned}
\mathsf{Adv}^{\text{ccs-2}}_{A,\Pi} &= 2 \cdot \Pr[B_2^{\mathcal{D}_{sk}}(x_0, x_1, s', y) = b] - 1 \\
&= \Pr[B_2^{\mathcal{D}_{sk}}(x_0, x_1, s', y) = 1 | b = 1] - \Pr[B_2^{\mathcal{D}_{sk}}(x_0, x_1, s', y) = 1 | b = 0] \\
&= (\Pr[\neg R(x_0, \mathcal{D}_{sk}(\alpha')) | b = 1] - \Pr[\neg R(x_0, \mathcal{D}_{sk}(\alpha')) | b = 0])/2 \\
&= (\Pr[R(x_0, \mathcal{D}_{sk}(\alpha')) | b = 0] - \Pr[R(x_0, \mathcal{D}_{sk}(\alpha')) | b = 1])/2 \\
&= (\mathsf{Succ}_{A,\Pi}(k) - \mathsf{Succ}_{A,A_2^*,\Pi}(k))/2 = \mathsf{Adv}^{\text{nm}}_{A,A_2^*,\Pi}(k)/2
\end{aligned}$$

Remarks

- This work showed that the original notion of *PA* was not right: to imply *CCS-2* (and even *NM*), the adversary needs access to an encryption oracle.

  Otherwise, one can construct a counter-example.

- Unfortunately, we also proved that *PA* cannot be achieved out of the random oracle model.

Conclusion

- This work achieves its goal: all the implications are proven as well as the gaps (separations).
- It remains an interesting open question to find an analogous but achievable formulation of Plaintext-Awareness for the standard model.