

# 公開鍵暗号の安全性

# 公開鍵暗号の安全性評価

- 公開鍵暗号の安全性は、攻撃者がどのような条件で攻撃をするのか(**Attack**)、その攻撃によってどのような安全性を保証するのか(どのようにしたら攻撃成功とみなす(**Goal**)のか)の2つの条件を定義して議論される。
- 攻撃(Attack)の種類は3種類
- 安全性(Goal)の種類は4種類
- 攻撃者は(**解読したい**)暗号文と公開鍵を知っている

# 攻撃法の分類

1. 選択平文攻撃(CPA; Chosen Plaintext Attack)  
攻撃者が任意の平文を選び、それに対応する暗号文を得られる(公開鍵暗号では常に可能な攻撃)
2. 選択暗号文攻撃(CCA1; Chosen Ciphertext Attack 1)  
攻撃者があらかじめ任意の暗号文に対する平文を入手できる
3. 適応的選択暗号文攻撃(CCA2; Chosen Ciphertext Attack 2)  
攻撃者はあらかじめ任意の暗号文に対する平文を入手でき、解読したい暗号文を入手した後も(その暗号文を除いて)任意の暗号文に対する平文を入手できる

# 安全性の定義

1. 一方向性 (OW; One-Wayness)  
暗号文  $C=E(M)$  から平文  $M$  を求めることができない
2. 強秘匿性 (SS; Semantically Secure)  
暗号文  $C=E(M)$  から  $M$  に関して 1bit の情報も分からない
3. 識別不可能性 (IND; Indistinguishability)  
暗号文  $C=E(M)$  について  $M=M_1$  or  $M_2$  であるとき、平文がそのどちらであるか識別できない
4. 頑強性 (NM; Non-Malleability)  
暗号文  $C=E(M)$  から平文  $M$  に関連する  $M'$  に対応する暗号文  $C'=E(M')$  を求められない

# (例) RSA暗号の安全性

1. 一方向性  
証明はされていないが一般に成り立つと仮定される
2. 強秘匿性  
平文Mの法Nに関するヤコビ記号(後述)の値を求めることができるので成り立たない
3. 識別不可能性  
候補平文を暗号化すれば容易に分かるので成り立たない
4. 頑強性  
平文の積に対応する暗号文は暗号文の積になるので成り立たない  
e.g.  $M_1^e \times M_2^e = (M_1 \times M_2)^e \pmod{N}$

# 公開鍵暗号の安全性評価の方法

- 攻撃法(3種類)と安全性(4種類)の組み合わせは12種類ある→どの組み合わせが最も厳密(厳しい基準)か？

		Attack		
		CPA	CCA1	CCA2
Goal	NM	NM-CPA	NM-CCA1	NM-CCA2
	IND	IND-CPA	IND-CCA1	IND-CCA2
	OW	OW-CPA	OW-CCA1	OW-CCA2

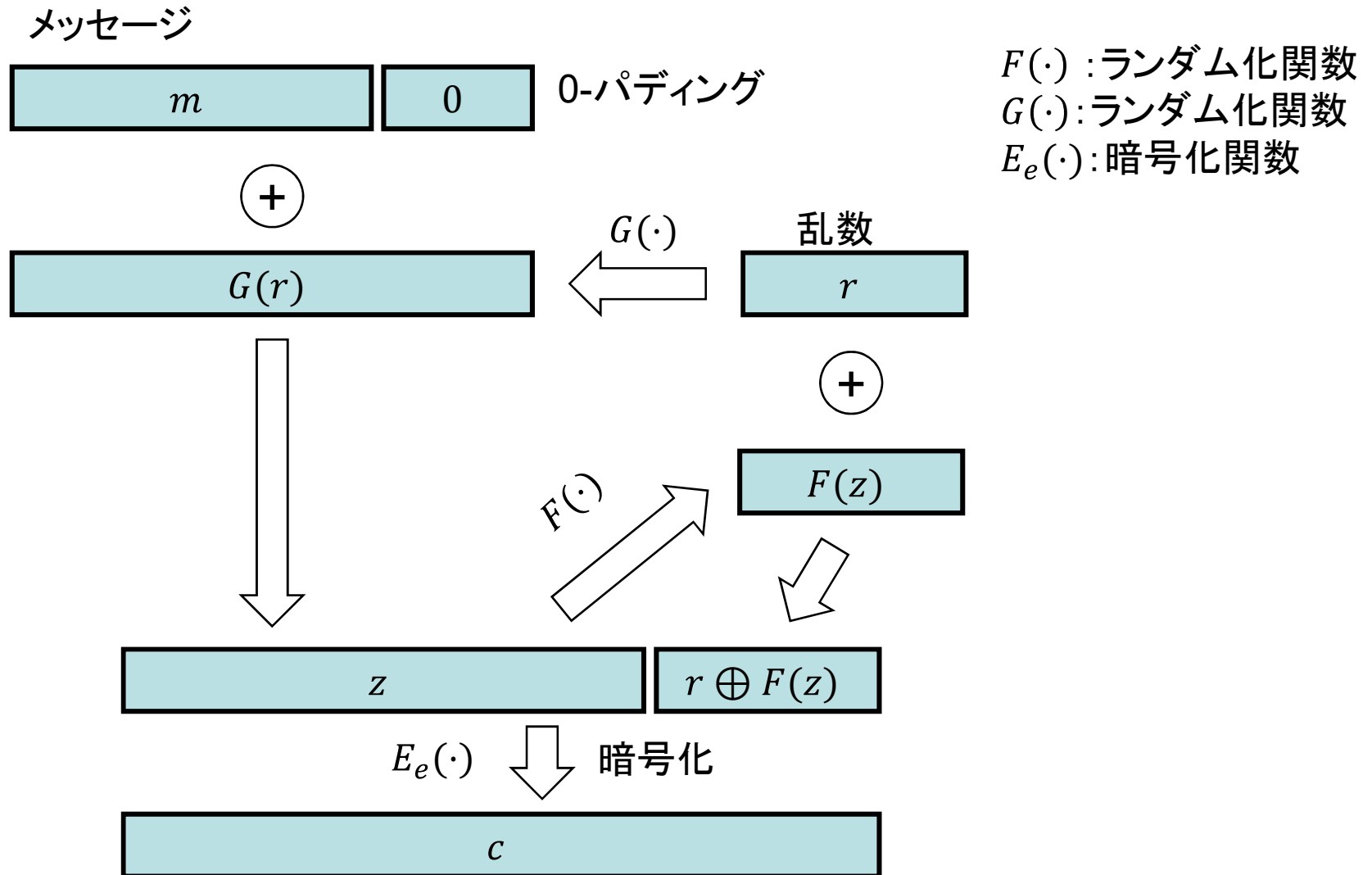
Diagram illustrating the relationships between security goals and attack types:

- Vertical arrows (downward) indicate that if a scheme is secure against a stronger attack, it is also secure against a weaker one (e.g., NM-CCA2 implies NM-CCA1 and NM-CPA).
- Horizontal arrows (leftward) indicate that if a scheme is secure against a stronger attack, it is also secure against a weaker one (e.g., IND-CCA2 implies IND-CCA1 and IND-CPA).
- A red circle highlights the **IND-CCA2** position, indicating it as the most stringent security goal.
- A red double-headed vertical arrow connects NM-CCA2 and IND-CCA2, indicating their equivalence in public-key cryptography.

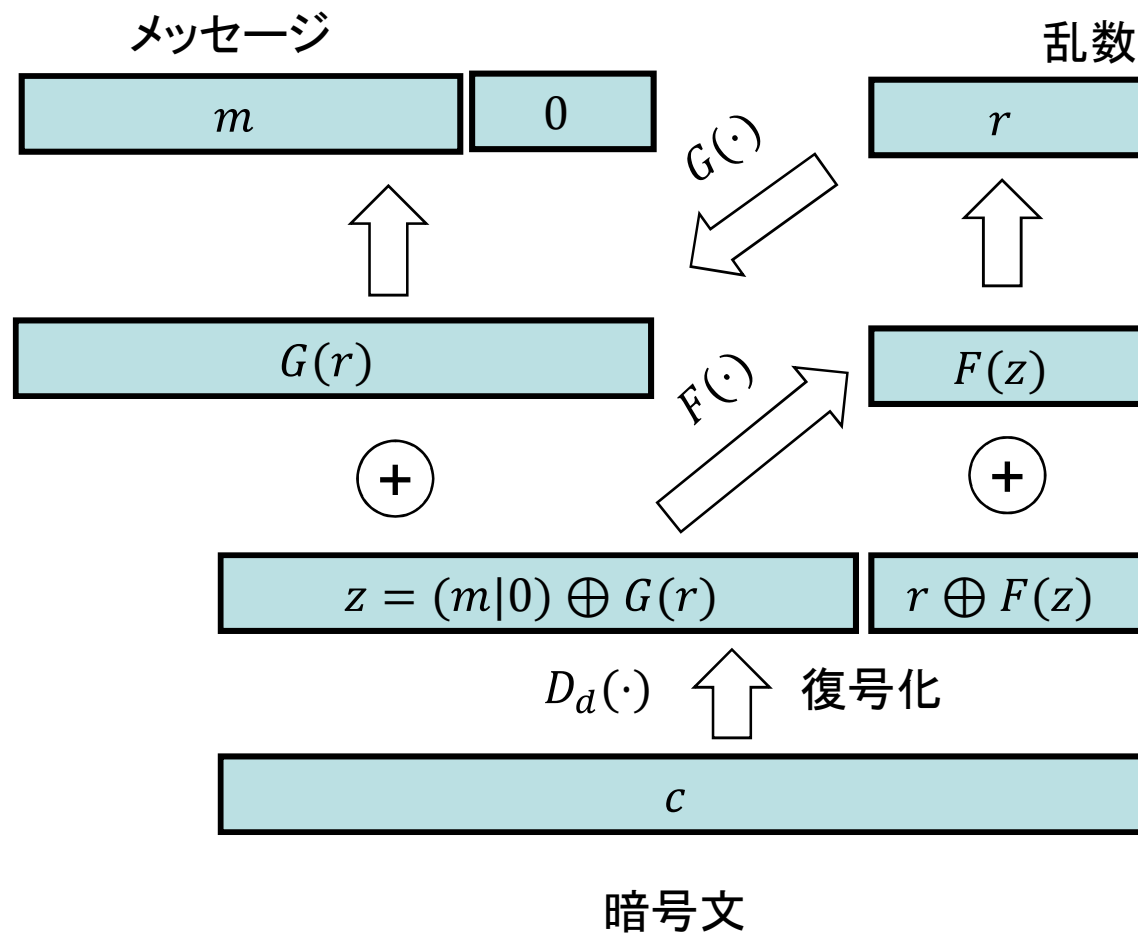
※INDとSSは公開鍵暗号では同値であることが証明されている

RSA暗号を**IND-CCA2**化した方式として、**RSA-OAEP**方式が提案され使われている

# RSA-OAEP暗号



# RSA-OAEP暗号(復号)



$F(\cdot)$  : ランダム化関数  
 $G(\cdot)$  : ランダム化関数  
 $D_d(\cdot)$  : 復号化関数