Bit Encryption is Complete for CCA2

Steven Myers @ Indiana University
abhi shelat @ University of Virginia

To appear FOCS 2009

Problem

- Given a public-key primitive that encrypts ONLY one-bit securely, can you encrypt k-bits securely?
- Trivial for CPA and CCA1 encryption: concatenate bit encryptions.
- Open question for CCA2 encryption since notion was introduced in [RS91].

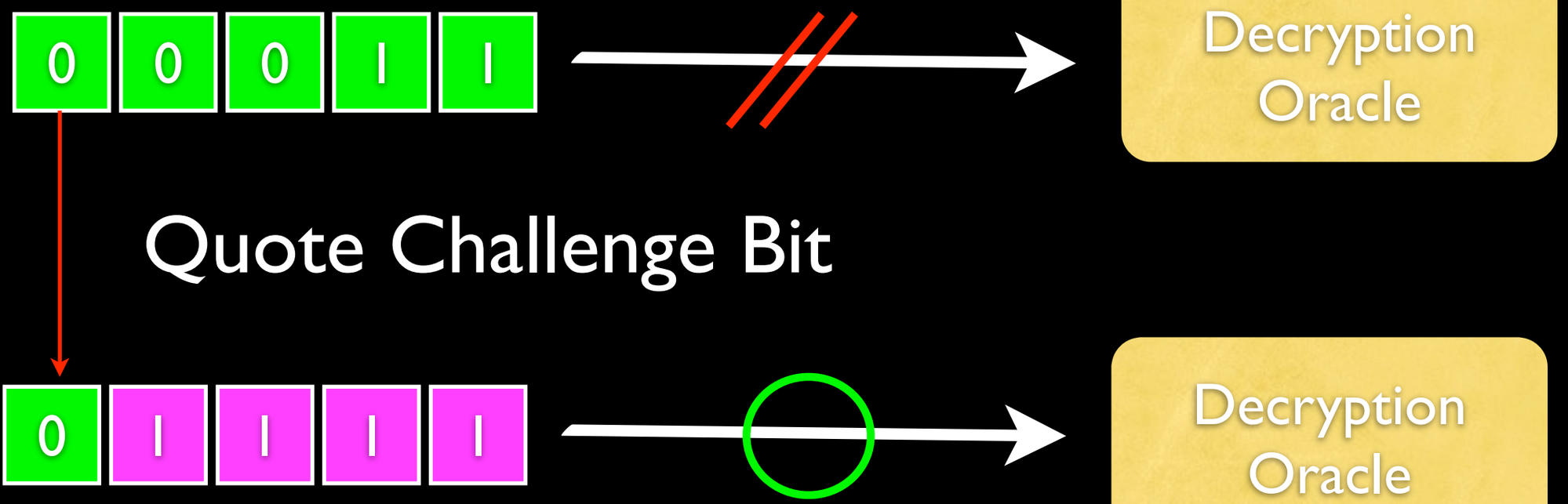
CCA2 Reordering Attacks

Challenge Ciphertext

Reordering Attack

CCA2 Quoting Attacks

Challenge Ciphertext



Reordering Attack

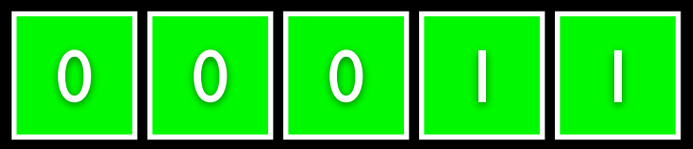
Construction Ideas

- Easy to deal with reordering attacks (e.g., encrypt each bit with a different public-key).
- Quoting attacks are harder to deal with.
- If you could guarantee there were no pasting attacks made, standard simulation arguments would work.
- Our construction prevents quoting attacks
- Actually build CCA2 KEM/DEM Scheme

Building Blocks

Inner PK Scheme

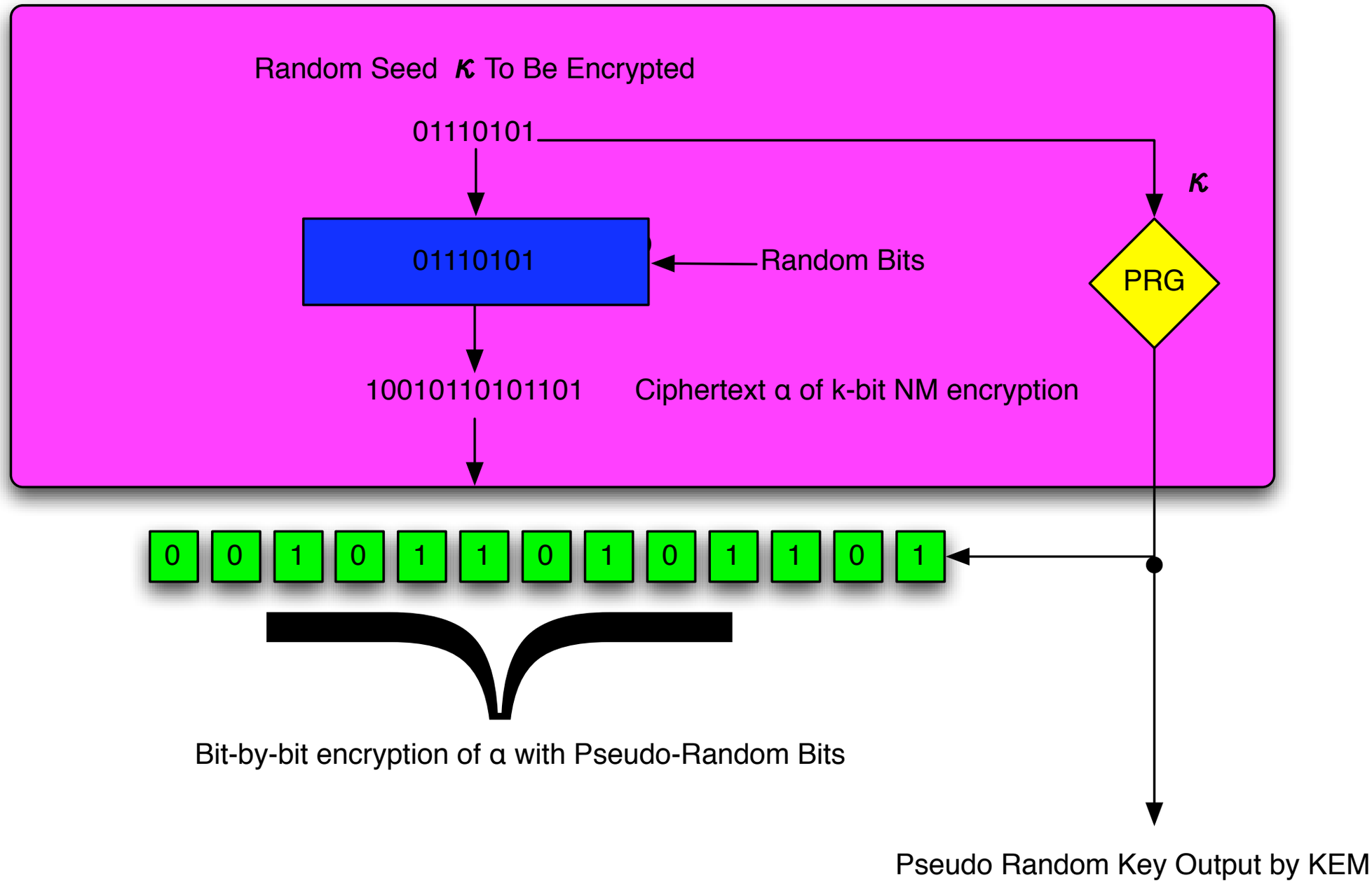
Outer PK Scheme



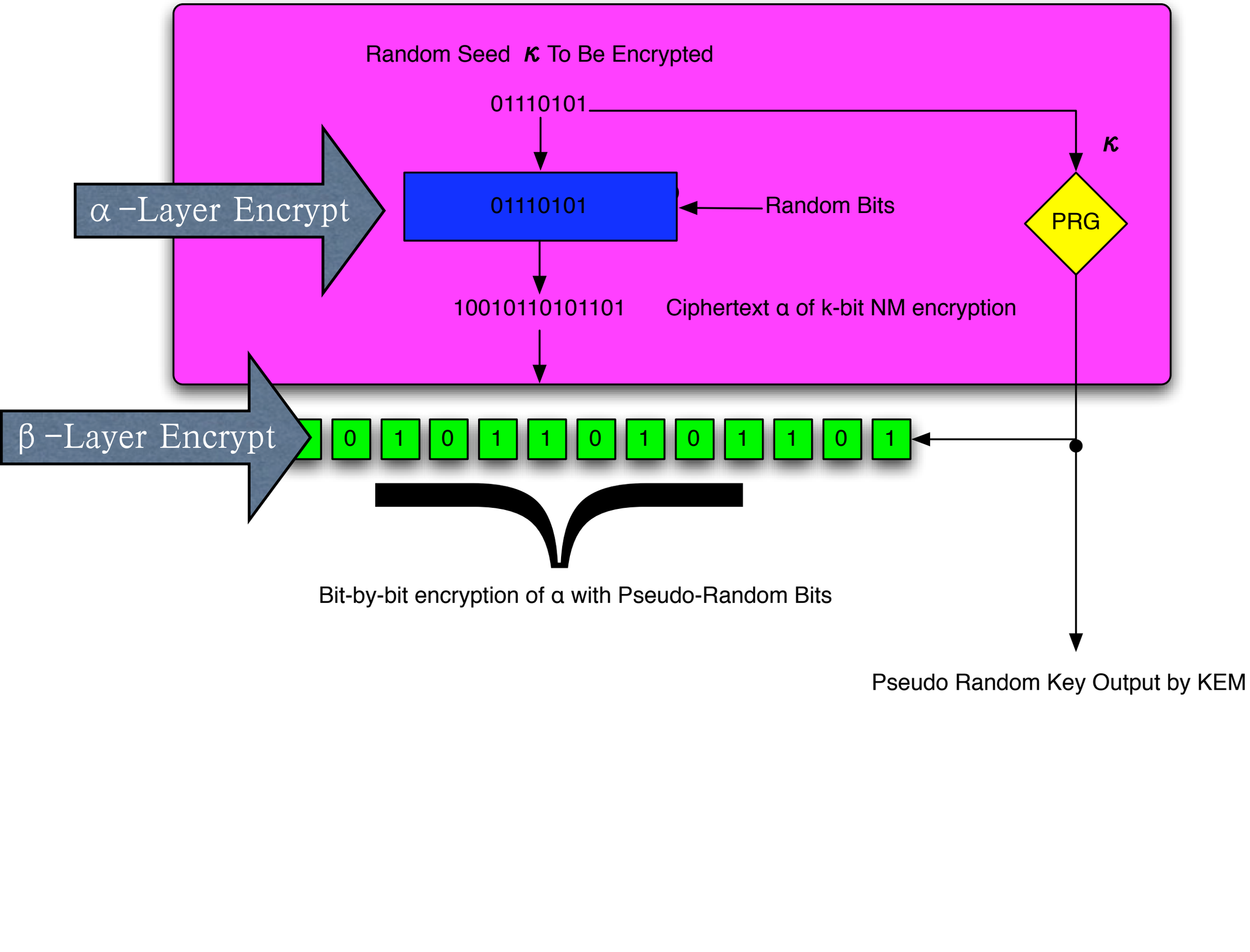
k-bit "weak" Non-Malleable Enc Scheme secure against non-quoting CCA2 adversary.

Concatenation of 1-bit CCA2 encryptions.

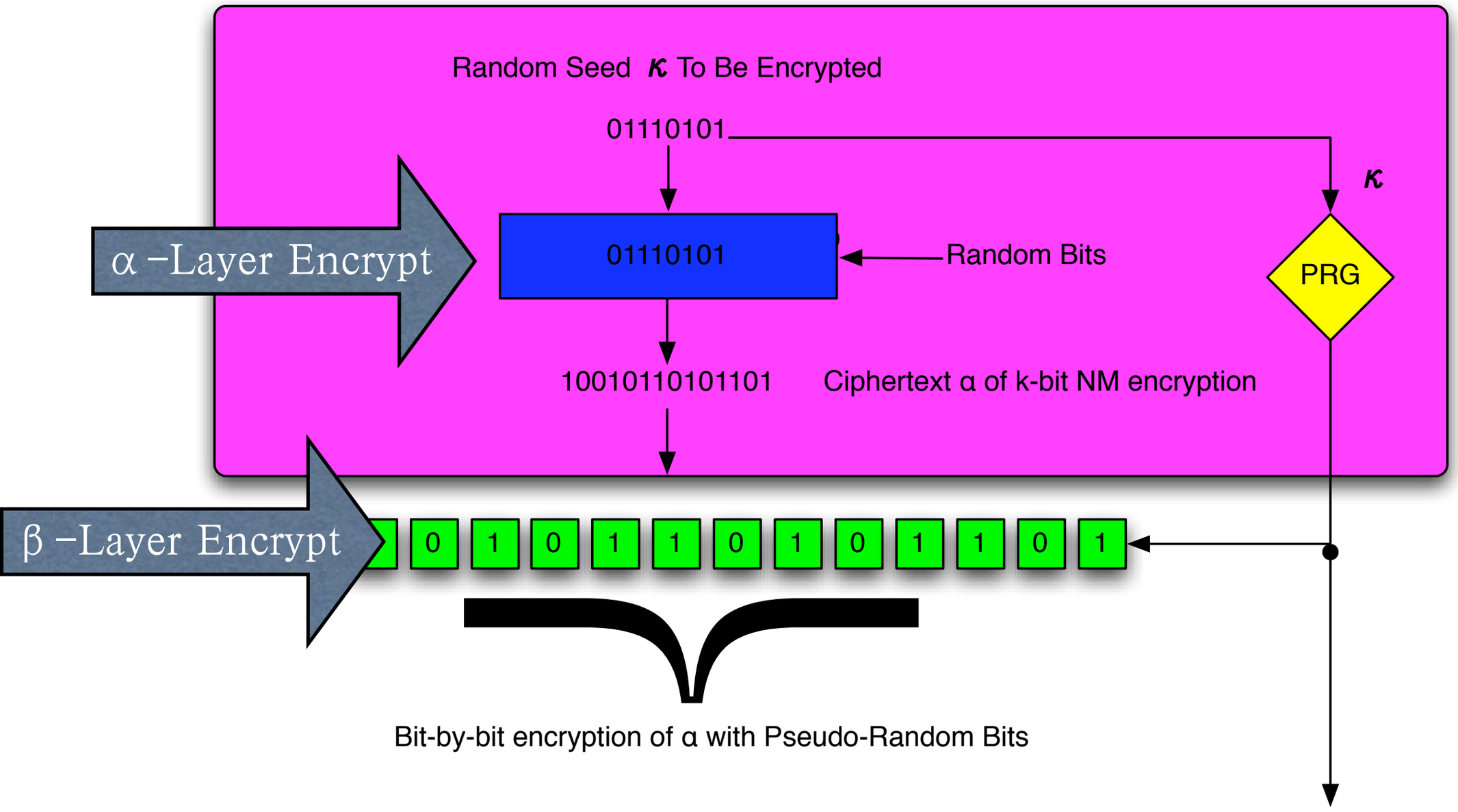
Many Bit CCA2 KEM Construction



Many Bit CCA2 KEM Construction

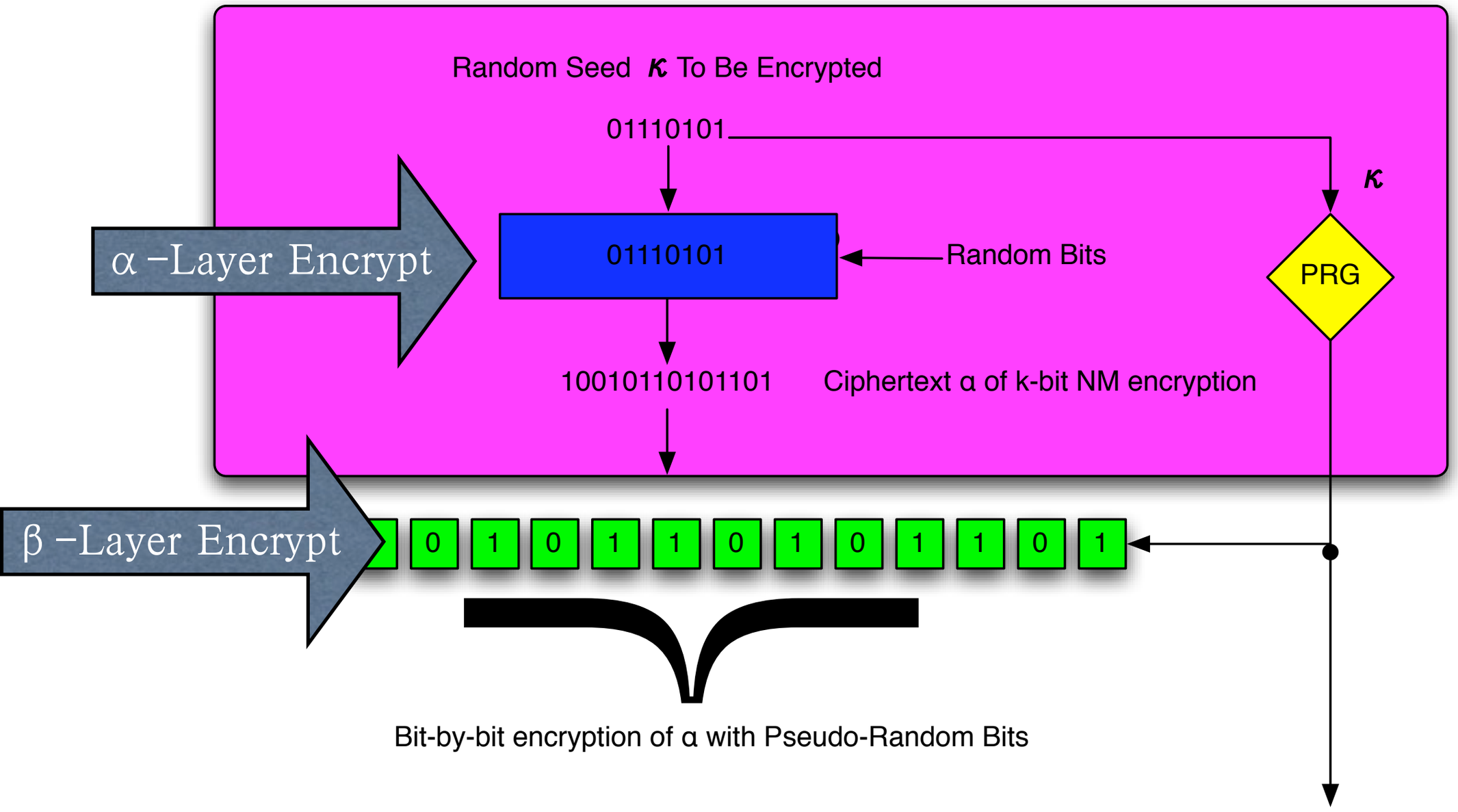


Many Bit CCA2 KEM Construction



Lemma 1: Adv cannot make α **−quotes before** β **−quotes.**

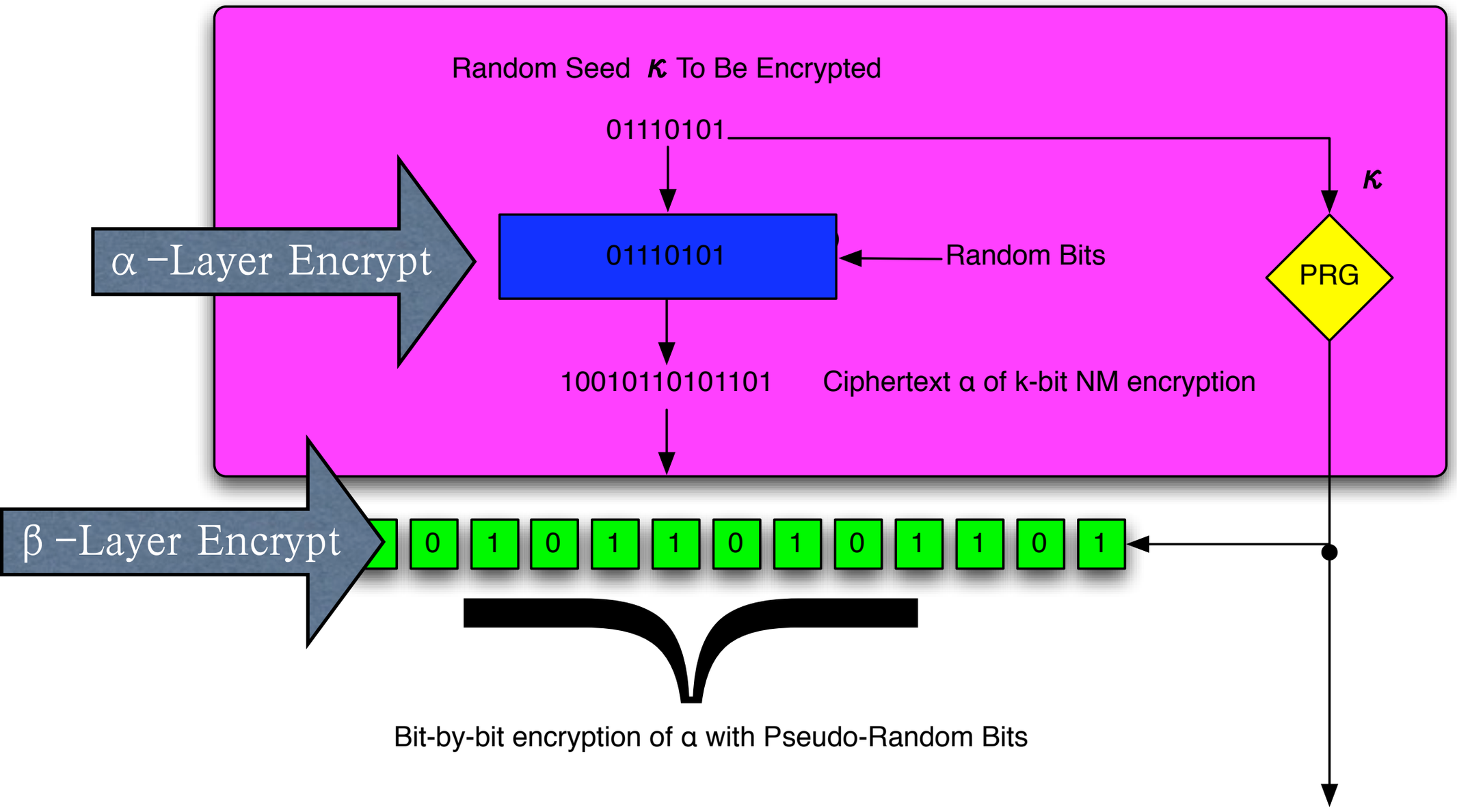
Many Bit CCA2 KEM Construction



Lemma 1: Adv cannot make α −quotes before β −quotes.

Lemma 2: Successful Adv must make β −quotes.

Many Bit CCA2 KEM Construction



Lemma 1: Adv cannot make α −quotes before β −quotes.

Lemma 2: Successful Adv must make β −quotes.

Lemma 3: Successful β −quote without preceding α −quote breaks non-malleability of α −layer.