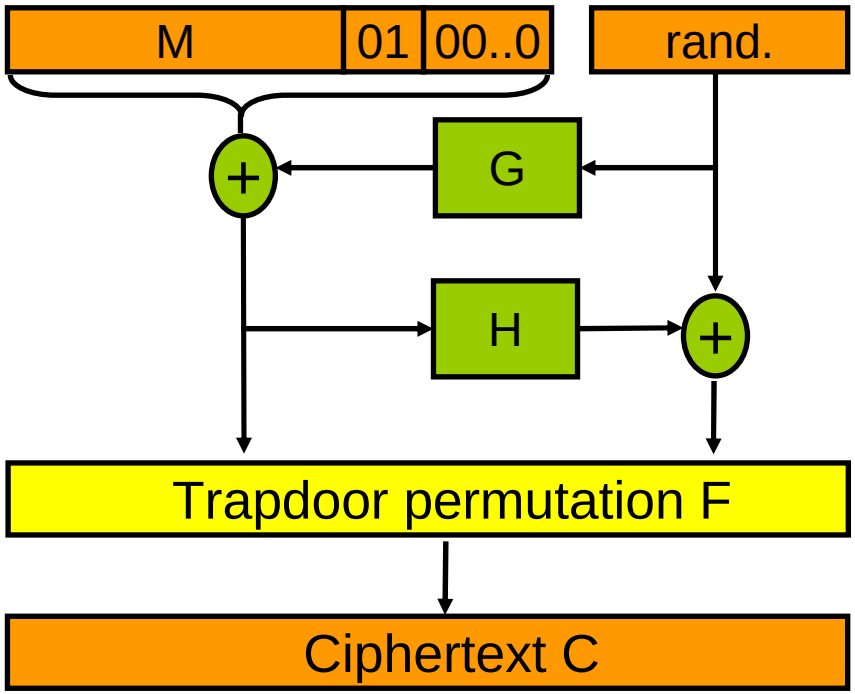
Security Proofs for OAEP in the Standard Model

Eike Kiltz & Adam O'Neill

OAEP padding



- **Optimal Asymmetric Encryption Padding**
  - Public-key encryption scheme by Bellare and Rogaway, 1994
- **RSA-OAEP**
  - Today's most used cryptosystem
  - PKCS V2.1, ANSI X9.44, ISO, IEEE, SET, …

Security of OAEP

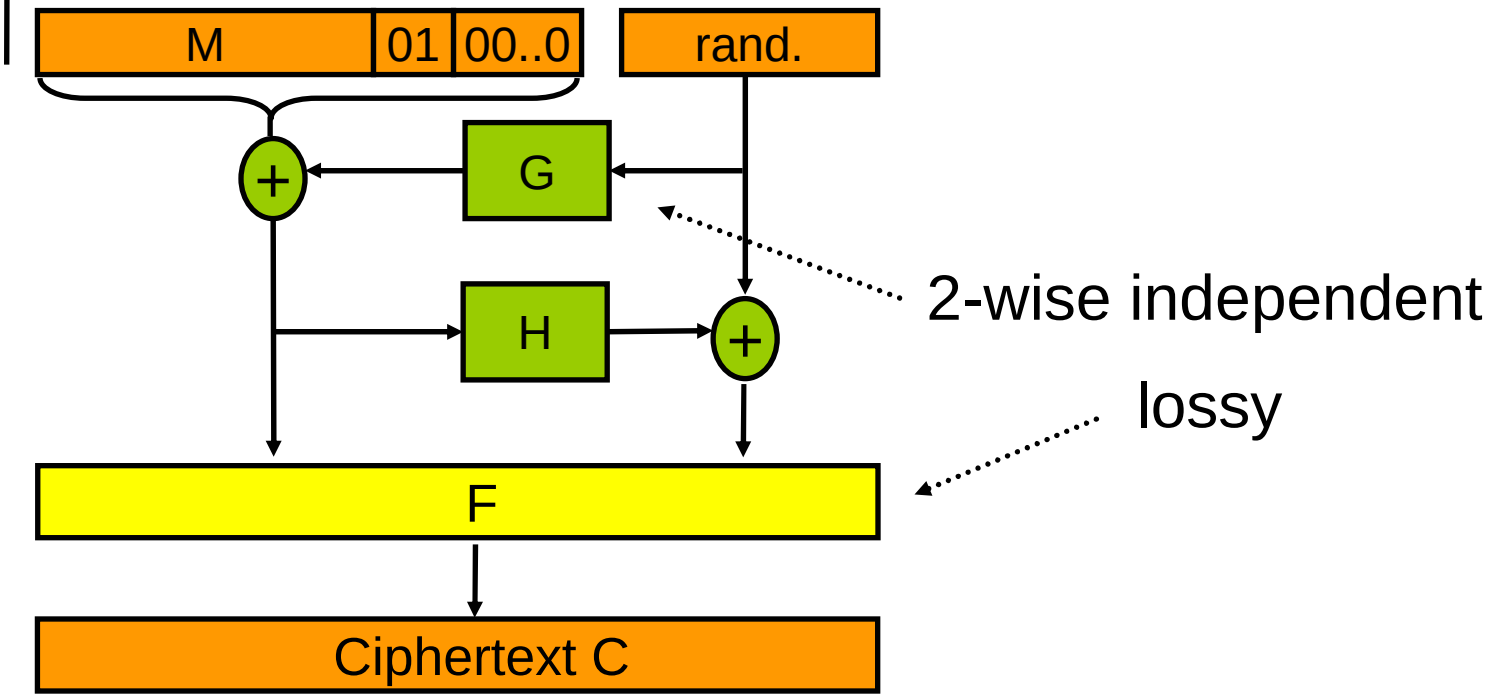
In the random oracle model:

- If F is one-way then F-OAEP is IND-CPA and plaintext-aware [BR94]
- RSA-OAEP is IND-CCA secure [FOPS01]

In the standard model:

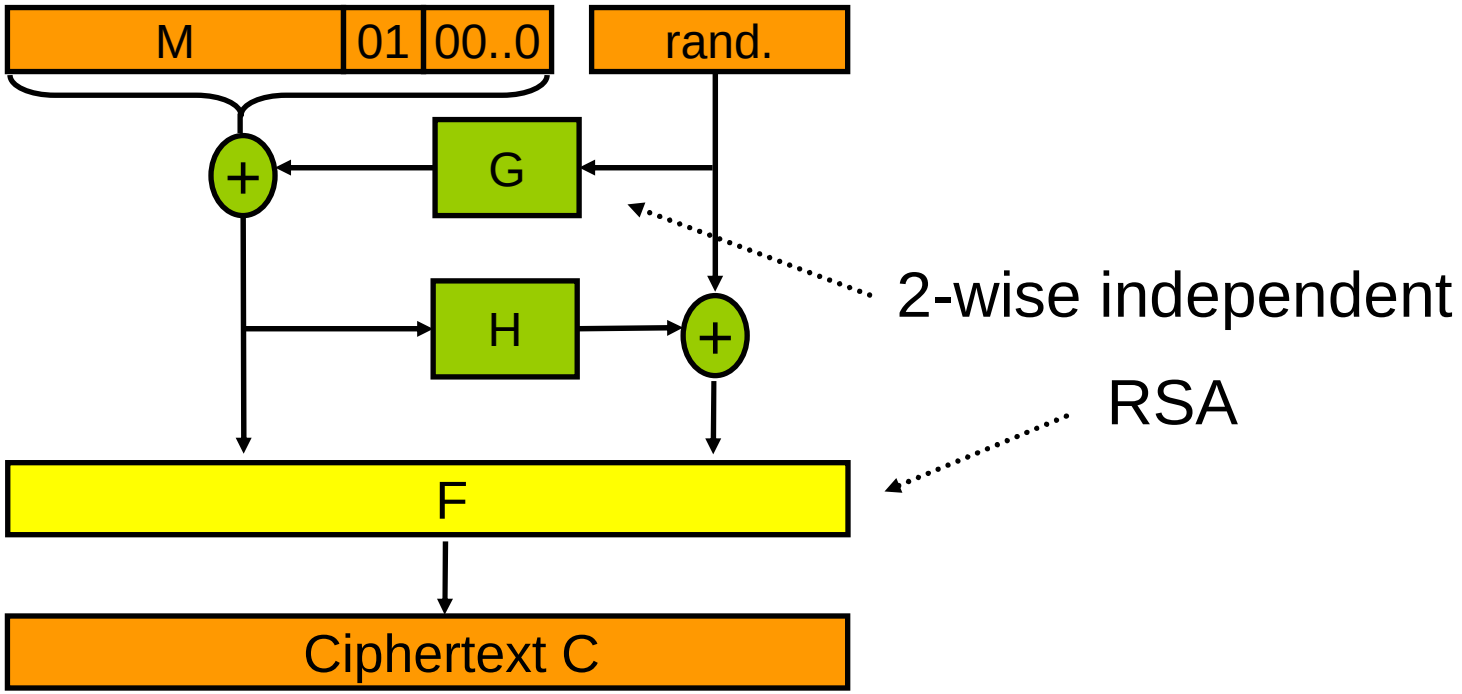
- IND-CCA security “provably unprovable” [Brown06], [BF05], [PV06], [KP09]

Main results (1)



Theorem: F = lossy trapdoor permutation
G = 2-wise independent.
⇒ F-OAEP semantically secure (IND-CPA)

Main results (2)



- **Φ-Hiding assumption [CMS99]**
- **Theorem:** RSA is lossy under Φ-Hiding assumption
- **Corollary:** RSA-OAEP is semantically secure (IND-CPA) under Φ-Hiding assumption