OAEP 3-Round
A Generic and Secure Asymmetric Encryption Padding

Duong Hieu Phan
ENS – France

David Pointcheval
CNRS-ENS – France

Asiacrypt '04

Jeju Island - Korea

December 6th 2004

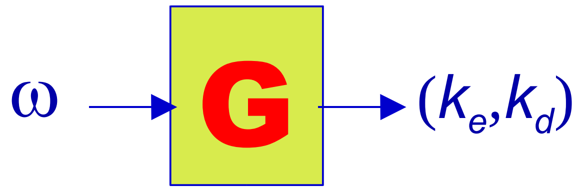
Summary

- Asymmetric Encryption
- OAEP 3-Round
  - Review
  - Limitations
- New Results
- Conclusion

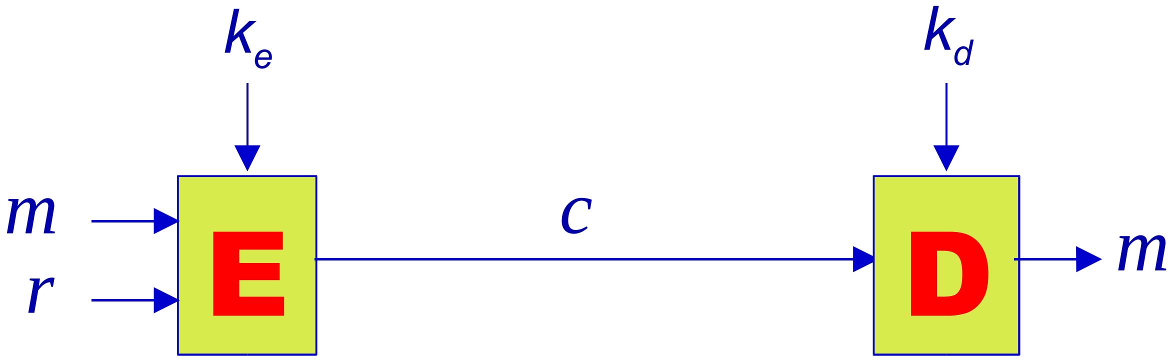
Asymmetric Encryption

An asymmetric encryption scheme π = (**G**,**E**,**D**) is defined by 3 algorithms:

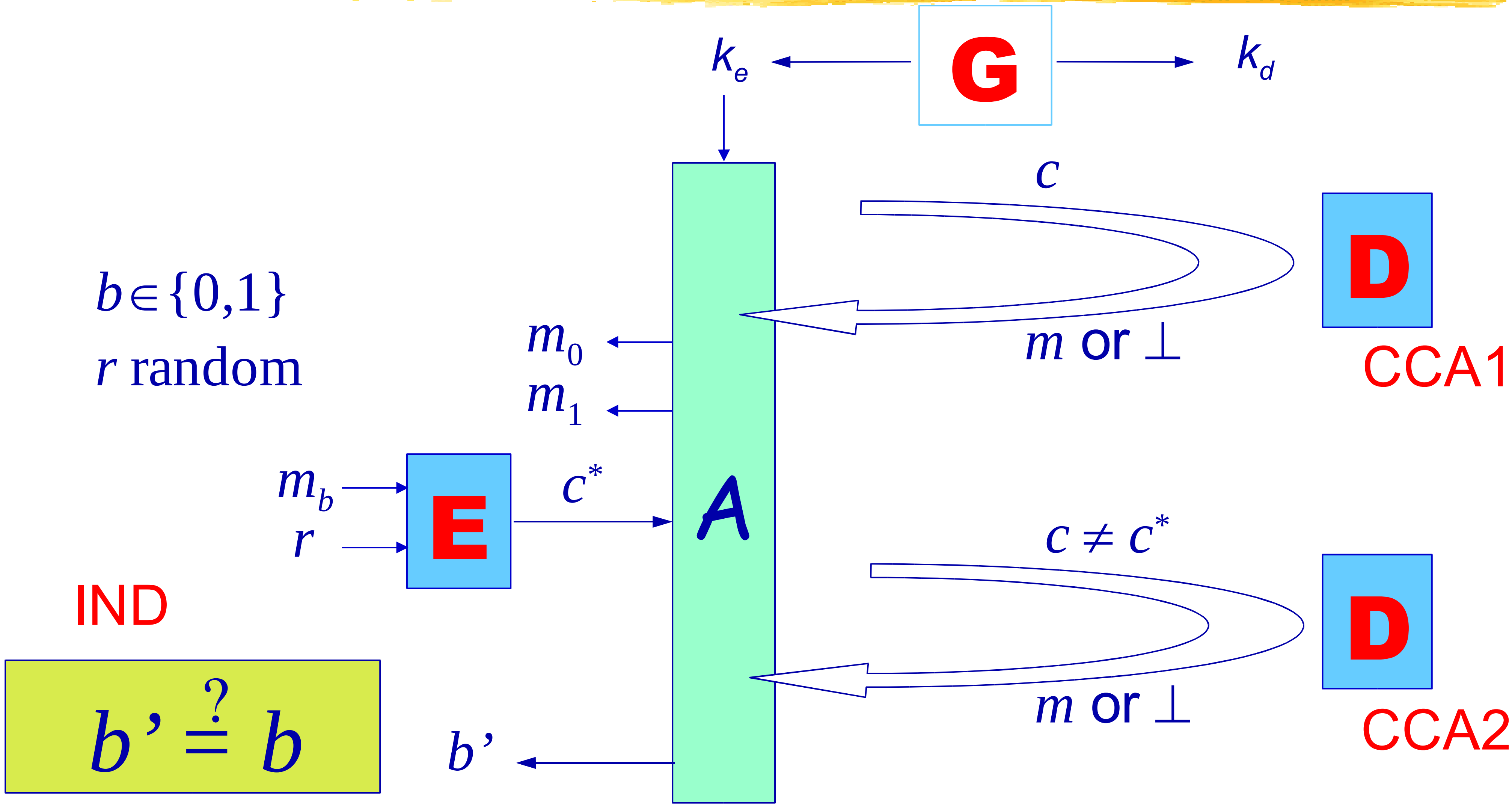
- **G** – key generation



- **E** – encryption
- **D** – decryption



Security Notion: IND-CCA2



IND: Probabilistic

- To achieve indistinguishability, a public-key encryption scheme must be probabilistic
  - otherwise, with the challenge $c = \mathbf{E}(m_b)$
  - one computes $c_0 = \mathbf{E}(m_0)$ and checks whether $c_0 = c$
- For any plaintext, the number of possible ciphertexts must be lower-bounded by 2^k, for a security level in 2^k :

at least $\mathrm{length}(c) \geq \mathrm{length}(m) + k$

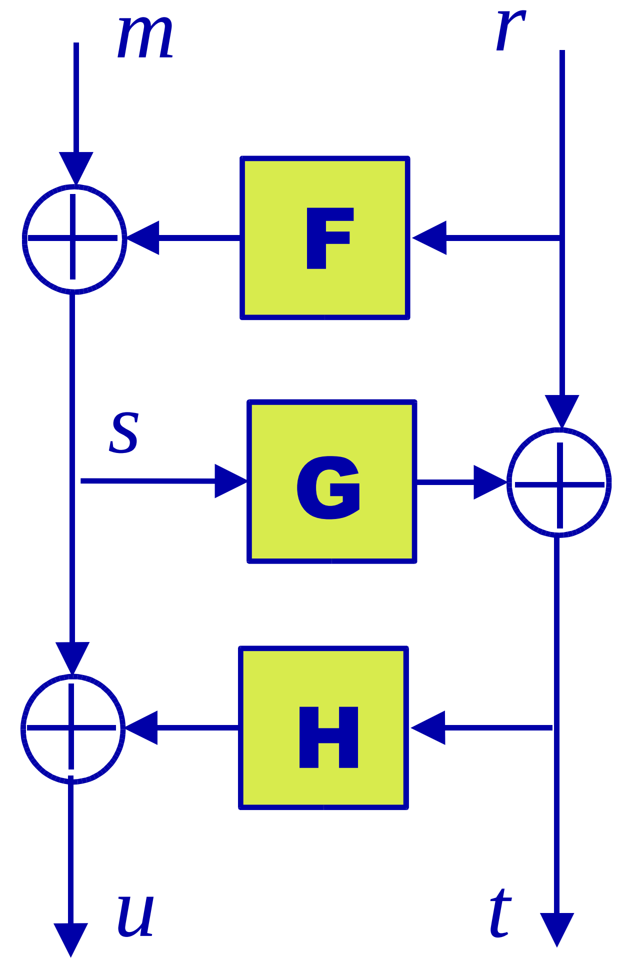
CCA: Redundancy?

- For IND-CCA2: redundancy
  Plaintext-awareness = invalid ciphertexts
- Last year, we proposed:
  - Full-Domain Permutation
  - OAEP 3-Round

  IND-CCA2 without redundancy

OAEP 3-Round

- **E**$(m) : c = f(t \| u)$
- **D**$(c) \; : t \| u = f^{-1}(c)$
  then invert OAEP, and return m



F, **G** and **H**: random functions

Security Result: Asiacrypt '03

With a random of size k_0, but no redundancy

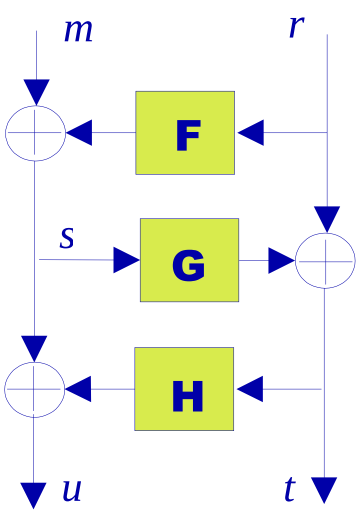
In the ROM, a (t,ε)-IND-CCA2 adversary helps to **partially invert** f within time $t' \approx t + q_{\mathbf{G}} q_{\mathbf{H}} T_f$, with success probability $\geq \varepsilon - q_{\mathbf{D}} Q / 2^{k_0}$

Limitations:

- Requires a trapdoor OW **permutation**
- Reduction to the **partial-domain one-wayness**

Intuition

- From the view of the challenge c^*
  - OAEP (with redundancy): [Sh01] showed that an adversary could produce a ciphertext c, with $r=r^*$
  - [FOPS01] ... but needs to query **H**(s^*)
  - OAEP 2-round (w/t redundancy): we thought that no easy proof could lead to **H**(s^*) but...
  - OAEP 3-round (w/t redundancy): could prove the requirement of the query **H**(t^*)
    $\Rightarrow$ **Partial-Domain OW**
- This paper: requirement of **both** **G**(s^*) and **H**(t^*) $\Rightarrow$ **Full-Domain OW**

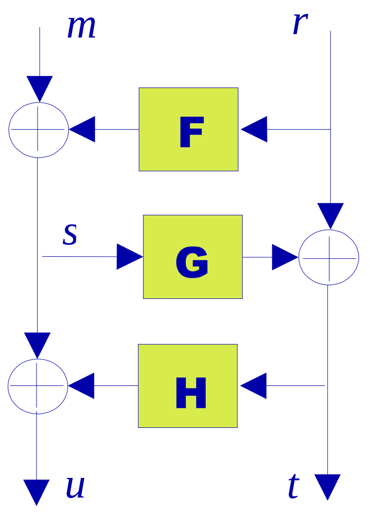


New Security Result

- With a random of size k_0, but no redundancy
- In the ROM, a (t,ε)-IND-CCA2 adversary helps to **invert** f within time $t' \approx t + q_{\mathbf{G}} q_{\mathbf{H}} T_f$, with success probability $\geq \varepsilon/2 - 5q_{\mathbf{D}} Q / 2^{k_0}$
- where Q is the global number of queries
- Simulation of the decryption oracle on c:
  - look for all the tuples $(s, \mathbf{G}(s), t, \mathbf{H}(t))$
  - check whether $f(t \,\|\, \mathbf{H}(t) \oplus s) = c$
  - compute $m = s \oplus \mathbf{F}(t \oplus \mathbf{G}(s))$ or random

Permutation Requirement

- The permutation requirement rules out many candidates: ElGamal, Paillier, Rabin, NTRU, ...
- Could we apply it to
  trapdoor one-way probabilistic injections?



- $f : (x,\rho) \rightarrow y = f\,(x,\rho)$
  - injection in x: at most one x for each y
    (but possibly many ρ)
  - hard to invert
  - a trapdoor helps to recover x

$$\mathbf{E}(m, r\|\rho) = f\,(t\|u, \rho)$$

Problems for the Simulation

- Simulation of the decryption oracle on c:
  - look for all the tuples $(s, \mathbf{G}(s), t, \mathbf{H}(t))$
  - check whether $f(t \,\|\, \mathbf{H}(t) \oplus s, \rho) = c$ (existence of ρ)
  - compute $m = s \oplus \mathbf{F}(t \oplus \mathbf{G}(s))$ or random
- Need of a decisional oracle: $\mathrm{Same}(c, c')$
  - Do c and c' encrypt the same element?
  - Computational problem given access to a decisional oracle $\rightarrow$ **Gap Problem**
- And what about $c = f(t^* \,\|\, \mathbf{H}(t^*) \oplus s^*, \rho)$?
  - $\mathrm{Same}(c, c^*)$ is true, but $m = m^*$ is unknown

Relaxed Chosen-Ciphertext Security

- [ADR02] *Generalized CCA*:
  - $\mathcal{R}$ is a decryption-respecting relation
    - Intuition: $\mathcal{R}$ formalizes a trivial relation between ciphertexts encrypting the same plaintext.
  - The adversary is not allowed to ask decryption queries on c in relation with c^*
- [CKN03] *Replayable CCA*:
  - On c which encrypts either m_0 or m_1: answer = TEST
- **Relaxed CCA**: $(m,r,\rho) \rightarrow c = \mathbf{E}(m,r\|\rho)$
  - On $c = \mathbf{E}(m^*,r^*\|\rho)$: answer = TEST

Relations

- *Generalized CCA*: is the most natural
  - non-significant bits in the ciphertext cannot be used in the attack.
- *Replayable CCA*: TEST reveals some information
- RCCA security $\Rightarrow$ Replayable CCA
  - a RCCA simulator decrypts more often
  - On $c = \mathbf{E}(m^*, r^* \| \rho) \Rightarrow m$ is m_b and thus either m_0 or m_1
- If $|\rho|=0$
  - TEST on c^* only: **RCCA = CCA**
  - Same is the equality test: **no** more Gap Problem

$\mathbf{E}(m, r \| \rho) = f\,(t \| u, \rho)$

Security Result

With a random of size k_0, but no redundancy

In the ROM, a (t,ε)-IND-RCCA adversary helps
to **invert** f within time $t' \approx t + q_D q_G q_H (T_f + T_{\mathrm{Same}})$
with success probability $\geq \varepsilon/2 - 5 q_D Q / 2^{k_0}$
after less than $q_D q_G q_H$ queries to the Same oracle

- quite loose reduction in general:
  - large security parameters
  - but small overhead: 160 bits of additional randomness

The RSA Case

- The same proof applies to RSA
  - RCCA = CCA
  - Gap-RSA = RSA
  - Proper bookkeeping: better reduction
    - $q_{\mathbf{D}} q_{\mathbf{G}} q_{\mathbf{H}} \rightarrow q_{\mathbf{G}} q_{\mathbf{H}}$

$\Rightarrow$ Cost of the reduction similar to OAEP
but relative to the Full-Domain RSA

$\Rightarrow$ The most efficient reduction
for an RSA-based padding into a $\mathbf{Z}_n^*$ element

Conclusion

OAEP 3-Round: the best OAEP-like variant

- the tightest reduction in the RSA case
  - for any exponent
  - relative to the RSA problem
- no redundancy: *almost* optimal bandwidth
- applicable to most of the asymmetric primitives
  - namely ElGamal, relative to the Gap DH