Chosen-Ciphertext Security without Redundancy

Duong Hieu Phan
ENS – France

David Pointcheval
CNRS-ENS – France

Asiacrypt '03
Taipei - Taiwan
December 1st 2003

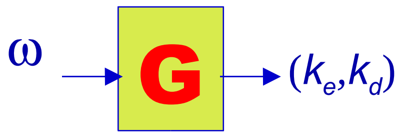
Summary

- Asymmetric Encryption
- Full-Domain Permutation Encryption
- 3-round OAEP
- Conclusion

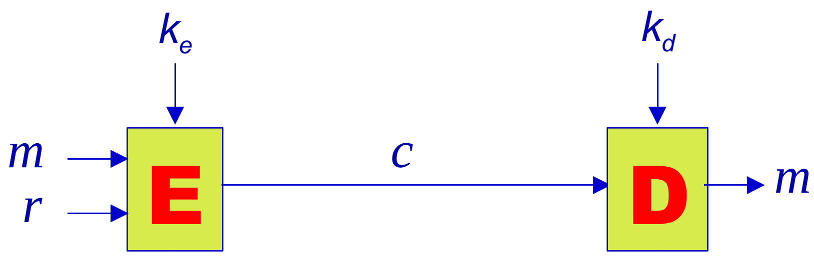
Asymmetric Encryption

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

- **G** – key generation



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



Security Notions

- **One-Wayness (OW) :**

  without the private key, it is computationally impossible to recover the plaintext

- **Semantic Security (IND - Indistinguishability) :**

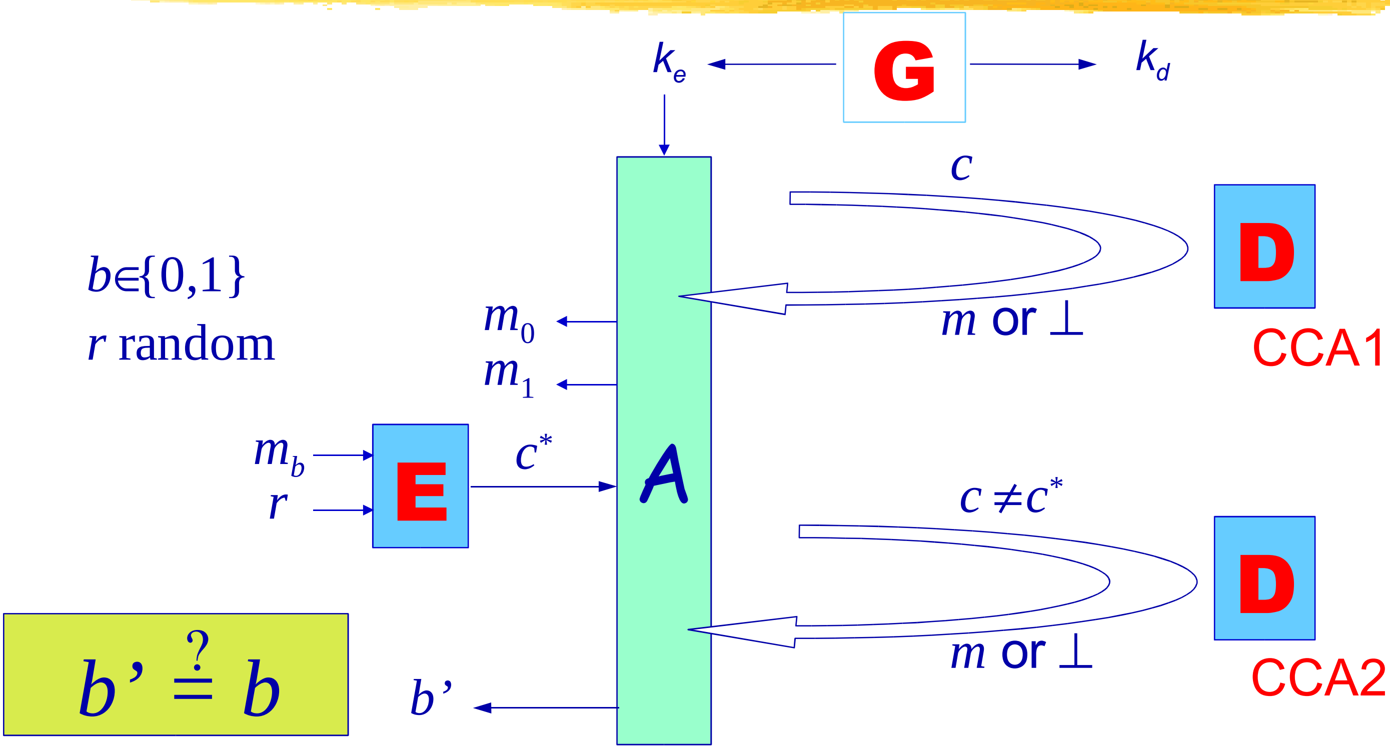
  the ciphertext reveals *no more* information about the plaintext to a **polynomial adversary**

Attacks

- **Chosen-Plaintext Attacks (CPA)**
  - the basic attack in the public-key setting
    - the adversary can encrypt any message of its choice
- More information: oracle access
- **Chosen-Ciphertext Attacks (CCA)**

  the adversary has access to the decryption oracle
  on any ciphertext of its choice (except the challenge)
  - non-adaptive (CCA1): only before receiving the challenge
  - adaptive (CCA2): unlimited oracle access

IND-CCA2



Indistinguishability: Probabilistic

To achieve indistinguishability, a public-key encryption scheme must be probabilistic

otherwise, with the chalenge $c = \mathbf{E}(m_b)$

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 $\mathbf{2^k}$:

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

Chosen-Ciphertext Security: Redundancy

To resist chosen-ciphertext attacks, all the proposed constructions introduce redundancy:

- OAEP: redundancy in the padding } *plaintext-awareness*
- REACT: MAC in the ciphertext } *plaintext-awareness*
- Cramer-Shoup: Proof of validity = redundancy

Such a redundancy makes that a random ciphertext is valid (a possible output of the encryption algorithm) with a very small probability, less than 2^{-k}:

in practice: at least $\mathrm{length}(c) \geq \mathrm{length}(m) + 2k$

Optimal Size = No Redundancy

- No redundancy = any ciphertext is valid:
  - is a possible output of $\mathbf{E}(m,r)$
  - the function $\mathbf{E}: \mathcal{M} \times \mathcal{R} \to \mathcal{C}$, $(m,r) \to c$ is a surjection
- Advantages:
  - optimal bandwidth
  - no reaction attack / implementation issues
  - easier distribution of the decryption process

Full-Domain Permutation Encryption

- First candidate: in the same vein as the Full-Domain Hash Signature
- Public permutation $\mathbf{P}$ (Random Permutation Model) onto $\mathcal{M} \times \mathcal{R} \approx \mathcal{C} \approx \{0,1\}^n \times \{0,1\}^k \approx \{0,1\}^l$
- Trapdoor one-way permutation f onto $\{0,1\}^l$

$$\mathbf{E}: \quad \mathcal{M} \times \mathcal{R} \to \mathcal{C}$$
$$(m,r) \to c = f(\mathbf{P}(m,r))$$

  - the public key is the pair $(f, \mathbf{P})$ which includes $\mathbf{P}^{-1}$
  - the private key is the trapdoor f^{-1}

FDP Encryption is IND-CCA2 Secure

In the RPM, a (t,ε)-IND-CCA2 adversary helps to invert f within almost the same time t, and with success probability greater than $\varepsilon - q/2^k$

- Simulation of the oracles **P**, **P**$^{-1}$ and **D** using a list **Λ** of tuples $\{(m,r,p,c)\}$: $p = \mathbf{P}(m,r)$, $c = f(p) = \mathbf{E}(m,r)$
  - problem if (m,r) is assumed to correspond to $\mathbf{P}^{-1}(f^{-1}(c))$ from the **D**-simulation, and the adversary asks for $\mathbf{P}(m,r)$:
    - the simulation should output $p = f^{-1}(c)$, which is unknown but **D** outputs m only: r is unpredictable

FDP Encryption: Properties

- No redundancy
- Optimal bandwidth: $\text{length}(c) = \text{length}(m) + k$
- High security level: IND-CCA2
  - with efficient reduction
  - but in the Random-Permutation Model

Can we weaken the assumptions?

The Random-Oracle Model

- A weaker model : the random-oracle model
  - access to a truly random function
- How to build a random permutation
  from a random function?
  - Luby-Rackoff: a Feistel construction
  - not that easy:
    here, one has access to the internal function...

  Let us try anyway: OAEP

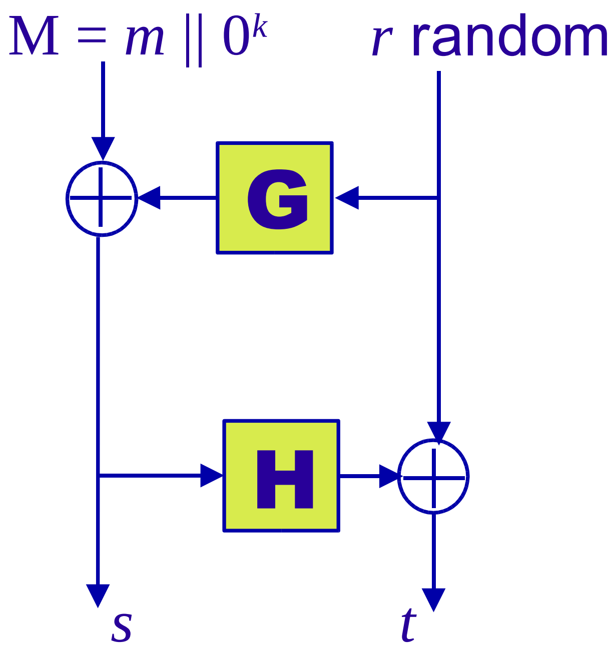
2-round OAEP

E(m) : $c = f(s \| t)$

D(c) : $s \| t = f^{-1}(c)$

then invert OAEP,

if the redundancy is satisfied, one returns m



G, **H**: random functions

2-round OAEP (cont'd)

- In the random-oracle model
- If f *is a trapdoor partial-domain OW permutation*:
  - $(s,t) \rightarrow f(s \,\|\, t)$ trapdoor one-way
  - $f(s \,\|\, t) \rightarrow s$ also hard to compute
- With a redundancy 0^k and random of size k_0

The encryption scheme f-OAEP:

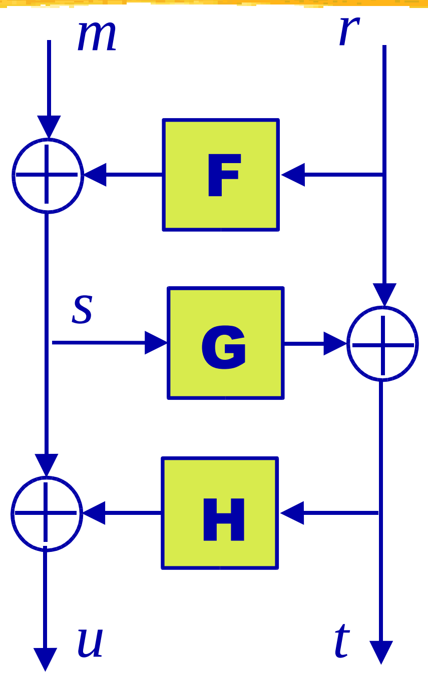
- IND-CCA2 with quadratic time reduction (in $q_F q_G T_f$)
  \+ quadratic lost (in $q_D q_G / 2^{k_0}$: $k_0 = 2k$)
- $\text{length}(c) = \text{length}(m) + 3k$

What About the Redundancy?

- For IND-CCA2: redundancy
  Plaintext-awareness = unvalid ciphertexts
- ***Without redundancy... is it still IND-CCA2?***
  - 2-round OAEP: no known attack, but no proof either
    - Any simulation seems to be subject
      to the Shoup's attack (malleability of OAEP)
  - 3-round OAEP: can be proven

3-round OAEP

- **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

Idea of the Security

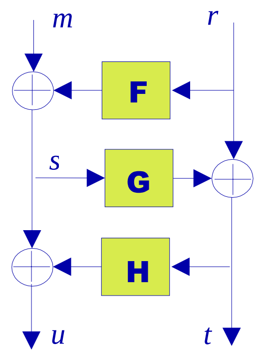
- 2-round OAEP: as in the Shoup's attack,
  - the adversary can forge a ciphertext c, with the same r as in the challenge ciphertext
  - the simulator cannot check that!
- With one more round:
  - the adversary is stuck!

$\Rightarrow$ one can simulate everything
  - at random when not already known

Tightness of the Reduction

- Everything works well with lists, Λ_F, Λ_G, Λ_H, Λ_D
- But for g = $\mathbf{G}(s)$, which implies
  - $\mathbf{F}(r) = m \oplus s$ for $r = t \oplus g$
  - for any $(t, h) \in \Lambda_H$, and $(m,c) \in \Lambda_D$
    such that $c = f(t, h \oplus s)$

  in case such a query is asked later



- Problem if such a query has already been asked...

Since g is random, the overall probability of such a bad event is upper-bounded by $q_D\, q_F / 2^k$.

Security Result

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 $t' \approx t + q_G q_H T_f$, and with success probability greater than $\varepsilon - q_D Q / 2^{k_0}$

The 3-round OAEP is:

- IND-CCA2 with quadratic time reduction
  + quadratic lost $(\Rightarrow k_0 = 2k)$
- $\mathrm{length}(c) = \mathrm{length}(m) + 2k$

Conclusion

We have proposed the first IND-CCA2 encryption schemes, without redundancy:

- the FDP encryption is optimal
  - based on the OW of the trapdoor permutation
  - optimal bandwidth
  - but in the Random-Permutation Model
- the 3-round OAEP has similar characteristics as the 2-round OAEP, but without redundancy