# *REACT: Rapid Enhanced-security Asymmetric Cryptosystems Transform*

## RSA Conference ' 2001
**San Francisco, California, April 2001**

**Tatsuaki Okamoto**
NTT
Yokosuka - Japan

**David Pointcheval**
ENS - CNRS
Paris - France

David.Pointcheval@ens.fr
http://www.di.ens.fr/users/pointche

---

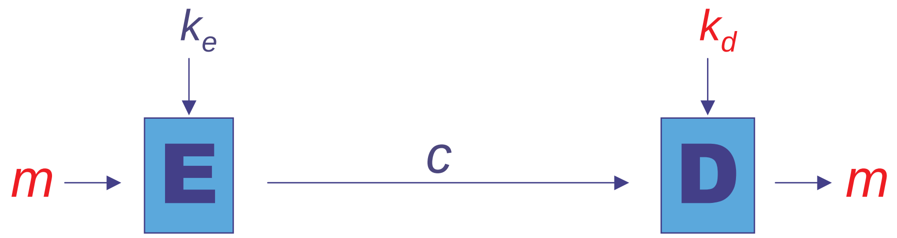
# Overview

- Introduction to Encryption
- Previous conversions
- REACT: the new conversion
  - Description
  - Security Result
- Conclusion

# Asymmetric Encryption

Encryption Algorithm **E** Encryption key $k_e$

Decryption Algorithm **D** Decryption key $k_d$




Security: it is impossible to get back $m$ just from $c$, $k_e$, **E** and **D** (without $k_d$)



# Security Notions

- the goals
  - One-Wayness
  - Semantic Security (Indistinguishability)
- the means/information available
  - Chosen-Plaintext Attacks
  - Chosen-Ciphertext Attacks

$\Rightarrow$ OW-CPA = weakest notion
IND-CCA = strongest notion

# Examples

- **RSA:** $n = pq$, $e$, public, $d = e^{-1} \bmod \varphi(n)$, secret

  $\mathbf{E}(m) = m^e \bmod n \qquad \mathbf{D}(c) = c^d \bmod n$

  **OW-CPA = RSA problem**

- **El Gamal:** $\mathbf{G} = (\langle g \rangle, \times)$, $y = g^x$, public, $x$ : secret

  $\mathbf{E}(m) = (g^a, y^a m) \qquad \mathbf{D}(c,d) = d/c^x$

  **OW-CPA = CDH problem**

  **IND-CPA = DDH problem**



# Generic Conversions

- Any trapdoor one-way (injective) function leads to a OW-CPA cryptosystem
- But OW-CPA not enough
- How to reach IND-CCA ?

  $\Rightarrow$ generic conversions
  from OW-CPA to IND-CCA

$(\mathcal{E},\mathcal{D})$ is assumed to be weakly secure and one designs a secure $(\mathbf{E},\mathbf{D})$

# Previous Conversions: OAEP

Bellare-Rogaway (EC ‘94) proposed **OAEP**, a very efficient conversion

- believed to provide a conversion of any *trapdoor OW* ***permutation*** into IND-CCA
- actually, it just provides a conversion of any *trapdoor* ***partial-domain*** *OW* ***permutation***

Anyway, RSA is the sole application

RSA-OAEP: **IND-CCA=RSA** [*FOPS’00*]

But the security reduction remains costly

$\Rightarrow$ no guarantee for actual parameters



# Recent Generic Conversions

Fujisaki-Okamoto (PKC ‘99)
from ***IND-CPA into IND-CCA***

Fujisaki-Okamoto (Crypto ‘99)
and Pointcheval (PKC ‘00)
from ***OW-CPA into IND-CCA***

Efficiency:

- efficient security reduction
- optimal encryption (just few more hashings)
- **non-optimal decryption** (1 re-encryption)

# New Conversion: REACT

PK-Cryptosystem $(\mathcal{E},\mathcal{D})$: $\mathcal{M} \times \mathcal{R} \rightarrow \mathcal{C}$

Block-Cipher $\mathbf{E}_k, \mathbf{D}_k : \{0,1\}^\lambda \rightarrow \{0,1\}^\lambda$

Hash functions G, H

$\mathbf{E}(m,r\|s) =$ $a = \mathcal{E}(r, s)$ with $r \in \mathcal{M}$, $s \in \mathcal{R}$

$b = \mathbf{E}_k(m)$ where $k = \mathrm{G}(r)$

$c = \mathrm{H}(m,r,a,b)$

$\mathbf{D}(a,b,c)$: Compute $r = \mathcal{D}(a)$ and $k = \mathrm{G}(r)$

extract $m = \mathbf{D}_k(b)$

if $c = \mathrm{H}(m,r,a,b)$ and $r \in \mathcal{M}$ then output $m$



# New Conversion: REACT

Efficiency:

- optimal encryption (just 2 more hashings)
- **optimal decryption** (just 2 more hashings)

Security: conversion

- in the random oracle model
- of any ***OW-PCA cryptosystem***
into an IND-CCA cryptosystem
- under the (weak) security of $(\mathbf{E}_k, \mathbf{D}_k)$

# Basic Security

- Plaintext Checking Attack (PCA):
  the adversary has access to an oracle which, on input a pair $(m,c)$, answers whether $c$ encrypts $m$, or not

  plain RSA: OW-PCA = RSA
  El Gamal: OW-PCA = GDH

- Weak security for $(\mathbf{E}_k, \mathbf{D}_k)$
  semantic security against passive attacks

  One-Time Pad: perfectly secure
  AES: very good security



# Applications

- El Gamal: OW-PCA = GDH
  $\Rightarrow$ REACT-El Gamal: IND-CCA=GDH
  *Rk*: On Elliptic Curves = PSEC-3

- RSA: OW-PCA = RSA
  $\Rightarrow$ REACT-RSA: IND-CCA=RSA
  *alternative to RSA-OAEP*

# REACT-RSA vs. OAEP-RSA

- Very efficient security reduction
  (much better than that
  of RSA-OAEP(+), SAEP+)

$\Rightarrow$ guarantees security for actual size (1024 bits)

- The (overall) security of the hybrid usage of RSA and symmetric encryption (e.g. AES) is theoretically guaranteed

  (No theoretical guarantee is given
  for the hybrid usage of OAEP-RSA)



# Hybridity

- Already very efficient with One-Time Pad
- Hybridity (use of AES, etc…)
  - makes it much more practical
  - security proof
- Enhanced hybridity:

  to encrypt many messages
  $a = \mathcal{E}(r, s)$ and $k = \mathrm{G}(r)$

  $b_i = \mathbf{E}_k(m_i)$ and $c_i = \mathrm{H}(m_i, r, a, b_i)$

# Conclusion

REACT is a new conversion:

- From any OW-PCA scheme, one makes an IND-CCA scheme
  - $\Rightarrow$ the best security level
- The cost is just:
  - 2 more hashings in encryption/decryption
  - $\Rightarrow$ almost optimal
- Can integrate symmetric encryption
  - $\Rightarrow$ improved efficiency