About Generic Conversions from any Weakly Secure Encryption Scheme into a Chosen-Ciphertext Secure Scheme

Tokyo University
November 24th 2000

David Pointcheval
Département d'Informatique
ENS - CNRS

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

Overview

- Introduction
- Security arguments
- Encryption
  - Security notions
  - Some examples
  - Previous conversions
  - REACT: new conversion
- Conclusion

Introduction

Tokyo University

November 24th 2000

David Pointcheval
Département d'Informatique
ENS - CNRS

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

Cryptography

Cryptography:

to solve security concerns

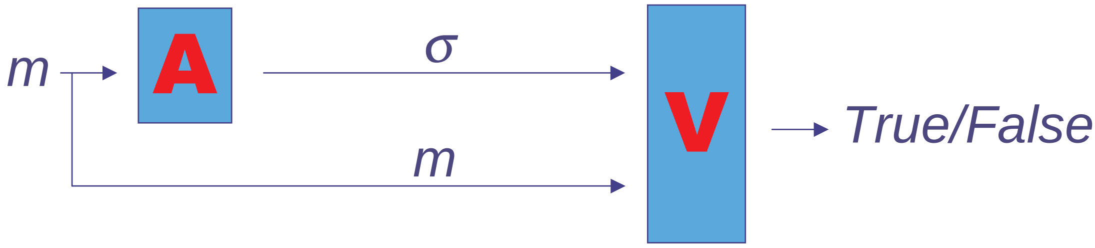
Authentication
Integrity
$\Rightarrow$ signature

Confidentiality $\Rightarrow$ encryption

Authentication/Integrity

Authentication Algorithm **A**

Verification Algorithm **V**

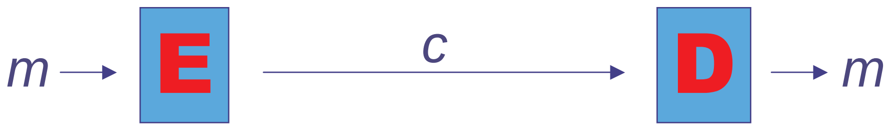


Security: it is impossible to produce a new valid pair (m,σ)

Encryption

Encryption Algorithm **E**

Decryption Algorithm **D**



Security: it is impossible to get back m just from c

Security Arguments

Tokyo University
November 24th 2000

David Pointcheval
Département d'Informatique
ENS - CNRS

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

Security Notions

Depending on the security concerns, one defines

- the goals that an adversary may would like to reach
- the means/information available to the adversary

Security Proofs

One provides a reduction from a "difficult" problem *P* to an attack *Atk*:

- *A* reaches the "prohibited" goals
  $\Rightarrow$ *A* can be used to break *P*
- no further hypothesis: standard model
- but that rarely leads to efficiency!
  $\Rightarrow$ some assumptions

Security Arguments

One provides a reduction from a "difficult" problem *P* to an attack *Atk*, under some ideal assumptions:

- ideal random hash function:
  random oracle model
- ideal symmetric encryption:
  ideal cipher model
- ideal group:
  generic model (generic adversaries)

Not perfect proofs $\Rightarrow$ security arguments

Encryption

Tokyo University
November 24th 2000

David Pointcheval
Département d'Informatique
ENS - CNRS

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

Asymmetric Encryption

Encryption Algorithm **E**
Decryption Algorithm **D**

Encryption key k_e
Decryption key k_d

$$m \rightarrow \underset{\downarrow k_e}{\boxed{\mathbf{E}}} \xrightarrow{\;c\;} \underset{\downarrow k_d}{\boxed{\mathbf{D}}} \rightarrow m$$

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

Security Notions

- Natural one: One-Wayness
- Perfect Security?:

  the ciphertext and public data do not reveal any information about the plaintext (but maybe the size)

  Information Theoretical sense $\Rightarrow$ Impossible

- Semantic Security (Indistinguishability):

  no polynomial adversary can learn any information about the plaintext from the ciphertext and public data (but the size)

Kinds of Attacks

- Chosen Plaintext: *(basic scenario)*

  in the public-key setting, any adversary can get the encryption of any plaintext of her choice (by encrypting it by herself)

- Chosen Ciphertext (adaptively):

  the adversary has furthermore access to a decryption oracle which decrypts any ciphertext of her choice (excepted the specific challenge!)

Required Security

- OW-CPA: *(basic level of security)*
  - enough in some scenarios
  - not enough in many others:
- CC-Attacks easy to perform

  $\Rightarrow$ attack to be made unuseful
- Plaintext-space often limited

  (“sell” - “buy” -- “yes” - “no” -- …)

  $\Rightarrow$ IND very often required

Main Security Notions

- OW-CPA: *(the weakest)*

$$\boxed{\Pr_{m,r}\left[\mathcal{A}(c) = m \,\middle|\, c = \mathbf{E}(m;r)\right]} \quad = \text{Succ negligible}$$

- IND-CCA: *(the strongest* - BDPR C ’98)

$$\boxed{2\Pr_{r,b}\left[\mathcal{A}_2^{\mathbf{D}}(m_0, m_1, c, s) = b \,\middle|\, \begin{matrix}(m_0, m_1, s) \leftarrow \mathcal{A}_1^{\mathbf{D}}(k_p) \\ c \leftarrow \mathbf{E}(m_b; r)\end{matrix}\right] - 1}$$

= Adv negligible

Example I: RSA Encryption

- $n = pq$, product of large primes
- e, exponent relatively prime to $\varphi(n) = (p-1)(q-1)$
- n, e : **public** key
- $d = e^{-1} \bmod \varphi(n)$: **secret** key

public $\mathbf{E}(m) = m^e \bmod n$

secret $\mathbf{D}(c) = c^d \bmod n$

OW-CPA = RSA problem

Example II: El Gamal Encryption

- $\mathbf{G} = (\langle g \rangle, \times)$ group of order q
- x : **secret** key
- $y = g^x$: **public** key

public $\mathbf{E}(m) = (g^a, y^a m) \rightarrow (c, d)$

secret $\mathbf{D}(c, d) = d / c^x$

OW-CPA = CDH problem
IND-CPA = DDH problem

Generic Conversions

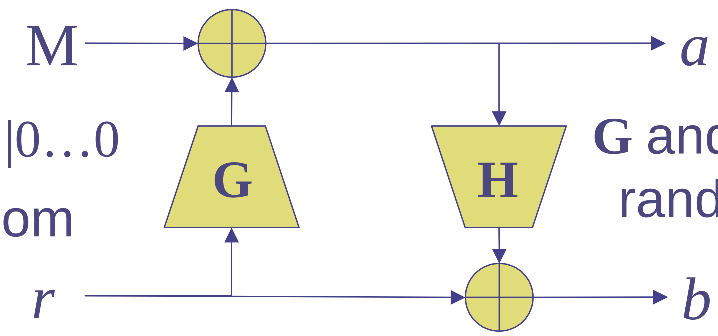
- Any trapdoor one-way (injective) function leads to a OW-CPA cryptosystem
- But OW-CPA not enough
- How to reach IND-CCA ?

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

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

Conversion: OAEP

Bellare-Rogaway EC '94: Feistel network:



$\mathrm{M} = m||0\ldots0$

r random

G and **H** random functions

E(m): Compute a,b and output $\mathcal{E}(a||b)$
D(c): Compute $a||b = \mathcal{D}(c)$
invert the Feistel network
and output m (*if the redundancy holds*)

OAEP (Cont'd)

It provides an optimal conversion of
any *trapdoor one-way* ***permutation***
into an IND-CCA cryptosystem

Efficiency: optimal (just 2 more hashings)

Application: RSA
(the sole candidate as
trapdoor one-way permutation!)

OAEP-RSA

$$\mathbf{E}(\mathrm{M},e) = \left(a = \mathrm{M} \oplus \mathrm{G}(r) \,||\, b = r \oplus \mathrm{H}(a)\right)^e \bmod n \rightarrow c \quad \text{for a random } r$$

guess 1 bit of M $\Leftrightarrow$ guess r $\Leftrightarrow$ guess a
$\Leftrightarrow$ guess (a,b) $\Leftrightarrow$ invert RSA

$$\mathbf{D}(c) = c^d \bmod n \rightarrow (a,b)$$
$$r = \mathrm{H}(a) \oplus b \text{ and } \mathrm{M} = a \oplus \mathrm{G}(r)$$
$$\text{if } \mathrm{M} = m||0\ldots0 \quad \text{then } m = x \text{ else "reject"}$$

valid ciphertext $\Leftrightarrow$ known plaintext
Plaintext Awareness

Conversion: FO 99

Fujisaki-Okamoto (PKC '99)

E$(m,s) = \mathcal{E}(m||s, \mathrm{H}(m||s))$
D(c): Compute $\mathrm{M} = \mathcal{D}(c)$
if $c = \mathcal{E}(\mathrm{M}, \mathrm{H}(\mathrm{M}))$
then split $\mathrm{M} = m||s$ and output m

conversion
of any ***IND-CPA cryptosystem***
into an IND-CCA cryptosystem

FO 99 (Cont'd)

Drawback:

based on an IND-CPA scheme
$\Rightarrow$ security relative to
decisional problems

Efficiency:

- optimal encryption (just 1 more hashing)
- non-optimal decryption (1 re-encryption)

Conversions: FO 99b, Po00

Fujisaki-Okamoto (Crypto '99)

Pointcheval (PKC '00)

$\mathbf{E}(m,r||s) = \mathcal{E}(r, \mathrm{H}(m||s)), \mathbf{E}_k(m||s)$ where $k = \mathrm{G}(r)$

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

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

if $a = \mathcal{E}(r, \mathrm{H}(\mathrm{M}))$

then split $\mathrm{M} = m||s$ and output m

Conversions

of any ***OW-CPA cryptosystem***

into an IND-CCA cryptosystem

FO 99b, Po 00 (Cont'd)

Advantage:

based on OW-CPA schemes

$\Rightarrow$ security relative to computational problems

Efficiency:

- optimal encryption (just 2 more hashings)
- non-optimal decryption (1 re-encryption)

Hybridity:

$(\mathbf{E}_k, \mathbf{D}_k)$ any symmetric encryption scheme

(weakly secure :

semantically secure against passive attacks)

New Conversion: REACT
(Okamoto-Pointcheval RSA '01)

E$(m,r\|s) =$ $a = \mathcal{E}(r, s)$ with $r \in \mathbf{G}$, $s \in \mathcal{R}$
$b = \mathbf{E}_k(m)$ where $k = G(r)$
$c = H(m,r,a,b)$

D(a,b,c): Compute $r = \mathcal{D}(a)$ and $k = G(r)$
extract $m = \mathbf{D}_k(b)$
if $c = H(m,r,a,b)$ and $r \in \mathbf{G}$ then output m

Conversion
of any ***OW-PCA cryptosystem***
into an IND-CCA cryptosystem

A New Attack: PCA

- Plaintext Checking Attack: the adversary
  - can get the encryption of any plaintext of her choice (by encrypting it by herself)
  - has furthermore access to an oracle which, on input a pair (m,c), answers whether c encrypts m, or not

Remark: IND-PCA cannot be achieved
$\Rightarrow$ we will just be interested in OW-PCA

Symmetric Encryption Scheme

One just need a symmetric encryption ($\mathbf{E}_k$, $\mathbf{D}_k$) semantically secure against passive attacks:

- One-Time Pad: perfectly secure ($\mathrm{Adv}^{\mathbf{E}} = 0$)
- Any classical scheme (DES, IDEA, AES,…)

  $\mathrm{Adv}^{\mathbf{E}} = \nu$ (very small)

Security Result

$$\mathrm{G} : \mathbf{G} \rightarrow \{0,1\}^{\ell_G} \quad \mathrm{H} : \{0,1\}^* \rightarrow \{0,1\}^{\ell_H} \quad \mathrm{E}_k : \{0,1\}^{\ell_E} \rightarrow \{0,1\}^{\ell_E}$$

If an adversary A against IND-CCA reaches an advantage $\mathrm{Adv}^{A} > \mathrm{Adv}^{\mathbf{E}}$ after q_{G}, q_{H} and $q_{\mathbf{D}}$ queries to G, H and $\mathbf{D}$ resp. one can break the OW-PCA of $(\mathcal{E},\mathcal{D})$ with probability greater than

$$\frac{\mathrm{Adv}^{A} - \mathrm{Adv}^{\mathrm{E}}}{2} - \frac{q_{\mathbf{D}}}{2^{\ell_H}}$$

Semantic Security (OTP)

Given (a,b,c) such that $a = \mathcal{E}(r,s)$,
$k = \mathrm{G}(r)$, $b = k \oplus m$, $c = \mathrm{H}(m,r,a,b)$

In order to guess the bit d such that $m = m_d$ an adversary has to ask either

- r to G to get k (and check b)
- (m_0,r,a,b) or (m_1,r,a,b) to H (and check c)

because of the randomness of G and H

Semantic Security (OTP Cont'd)

Probability that r $(= \mathcal{D}(a))$ has been asked to G or H greater than $\mathrm{Adv}^{A}/2$

Simply find the good one with the PC-oracle,
to all the G queries and the H queries
$\Rightarrow q_{\mathrm{G}} + q_{\mathrm{H}}$ queries to the PC-oracle

Plaintext Extractor

(a,b,c) valid ciphertext $\Rightarrow$ one has asked
for (m,r,a,b) to H to get a valid c
or has guessed c,
but with probability less than $1/2^{\ell_H}$

Plaintext Extractor

The plaintext extractor, to decrypt a given ciphertext (a,b,c), looks for any query (m,r,a,b) to H such that

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

and checks whether

- $r = \mathcal{D}(a)$ (thanks to the PC-oracle)
- $b = \mathbf{E}_k(m)$ for $k = \mathrm{G}(r)$

Correct extraction with probability greater than $1 - 1/2^{\ell_H}$

CCA Security

After q_D queries to the decryption oracle

- all the decryptions are correctly simulated with probability greater than

$$(1 - 1/2^{\ell_H})^{q_D} \geq 1 - q_D/2^{\ell_H}$$

- r has been asked to G or H
(and thus extracted using the PC-oracle)
with probability greater than

$$\boxed{\frac{\mathrm{Adv}^A}{2} - \frac{q_D}{2^{\ell_H}}}$$

The Diffie-Hellman Problems

- computational
  - Given $A=g^a$ and $B=g^b$
  - Compute DH(A,B) = $C=g^{ab}$
- decisional
  - Given A, B and C in $<g>$
  - Decide whether C = DH(A,B)
- Gap

  Solve the computational problem, with access to a decisional oracle

Intractability of the Gap-DH (Okamoto-Pointcheval PKC '2001)

The Computational Diffie-Hellman problem is believed intractable for suitable groups

Gap-DH easy $\Rightarrow$ D-DH = C-DH

D-DH easy $\Rightarrow$ G-DH = C-DH

C-DH is believed strictly stronger than D-DH $\Rightarrow$ G-DH intractable

Recall: El Gamal Encryption

- **G** $= (<g>, \times)$ group of order q
- x : **secret** key
- $y=g^x$: **public** key

public $\mathbf{E}(m) = (g^a, y^a m) \rightarrow (c, d)$

secret $\mathbf{D}(c, d) = d / c^x$

OW-CPA = CDH problem

IND-CPA = DDH problem

OW-PCA = GDH problem

PSEC - 3

- **G** is any group, and g of order q
- G and H: two hash functions
- **E**, **D**: symmetric encryption scheme

x : **secret** key
$y=g^x$: **public** key

E(m): $a \leftarrow_R \mathbf{Z}_q,\ R \leftarrow_R \mathbf{G}$
$A \leftarrow g^a,\quad A' \leftarrow R\, y^a$
$k \leftarrow \mathrm{G}(R),\ B \leftarrow \mathbf{E}_k(m),$
$C \leftarrow \mathrm{H}(R, m, A, A', B)$

$\longrightarrow (A, A', B, C)$

D(A, A', B, C): $R \leftarrow A'/A^x,$
$k \leftarrow \mathrm{G}(R),\ m \leftarrow \mathbf{D}_k(B),$
check whether $C = \mathrm{H}(R, m, A, A', B)$

Properties of PSEC-3

- this is a new EG-scheme:
  - OW-CPA = C-DH (+ROM)
  - OW-PCA = Gap-DH (+ROM)
  - IND-CCA = Gap-DH (+ROM)
- hybridity: one can integrate
  any symmetric encryption scheme,
  semantically secure
  against passive attacks
  (a very weak notion of security)

e.g. the one-time pad, AES, etc…

Efficiency

It just requires 2 exp./Enc, and 1 exp./Dec

$\Rightarrow$ one of the most efficient variant

Other variants:

- Tsiounis-Yung (PKC ‘98) D-DH + ROM + Other = Jakobsson-Schnorr (AC ‘00) ROM + GM
  3 exp./Enc - 3 exp./Dec
- Shoup-Gennaro (EC ‘98) D-DH + ROM
  5 exp./Enc - 7 exp./Dec
- Cramer-Shoup (Crypto ‘98) D-DH
  5 exp./Enc - 3 exp./Dec

Efficiency (Cont’d)

Recent variants:

- PSEC-1 (Fujisaki-Okamoto - PKC ‘99)
  D-DH + ROM
  2 exp./Enc - 3 exp./Dec
- PSEC-2 (Fujisaki-Okamoto - Crypto ‘99)
  C-DH + ROM
  2 exp./Enc - 3 exp./Dec
- DHAES (Abdalla-Bellare-Rogaway)
  New assumption DH-Oracle (RSA ‘2001)
  similar to DDH + ROM
  + MAC
  2 exp./Enc - 1 exp./Dec

More About Efficiency

$\mathbf{E}(m,r\|s) = \quad a = \mathcal{E}(r, s)$

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

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

To encrypt many messages:

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

$b_1 = \mathbf{E}_k(m_1)$ and $c_1 = \mathrm{H}(m_1,r,a,b_1)$

…

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

with just a semantically secure symmetric encryption against passive attacks

Conclusion

Tokyo University

November 24th 2000

David Pointcheval
Département d'Informatique
ENS - CNRS

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

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