New Public Key Cryptosystems based on the Dependent–RSA Problems

David Pointcheval

Laboratoire d'Informatique
École Normale Supérieure

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

Summary

Public Key Cryptosystems

Alice sends a ciphertext to Bob

Only Bob can recover the plaintext

$\Longrightarrow$ confidentiality

- To recover the plaintext
  = to find the whole plaintext?
  = to get some information about it?
- Which means can be used?
  = Just the public key
  = Some extra informations

Security Notions

One-Wayness:
from the ciphertext, one cannot recover the whole plaintext without the secret key

Semantic Security, aka Indistinguishability [GM84]:
from the ciphertext, one cannot get any information about the plaintext

Non-Malleability [DDN91]:
from the ciphertext, one cannot derive a new ciphertext whose plaintexts are related.

Attacks

Chosen-Plaintext Attacks:
the attacker can encrypt any plaintext of her choice
(that can be done with any public-key cryptosystem)

Chosen-Ciphertext Attacks (lunchtime [NY90], adaptive [RS91]):
the attacker has furthermore access to a decryption oracle
with some restriction

$$\text{OW-CPA} \Leftarrow \text{Ind-CPA} \Leftarrow \text{Ind-CCA} \Leftrightarrow \text{NM-CCA}$$

Previous Schemes

	RSA 78	EG 85	OAEP 94	OU 98	NS 98	CS 98
OW-CPA	RSA	DH	RSA	Fact	HR	DH
Ind-CPA	–	DDH	RSA	HR	HR	DDH
Ind-CCA	–	–	RSA	–	–	DDH

OAEP is designed in the Random Oracle Model
and is the most efficient scheme.

The Dependent–RSA Problems

- the Computational (C-DRSA(N, e)):
  given $\alpha = a^e \bmod N$,
  find $\beta = (a+1)^e \bmod N$
- the Decisional (D-DRSA(N, e)):
  given $\alpha = a^e \bmod N$ and $\beta = b^e \bmod N$,
  decide whether $b = a + 1 \bmod N$
- the Extraction (E-DRSA(N, e)):
  given $\alpha = a^e \bmod N$ and $\beta = (a+1)^e \bmod N$,
  find $a \bmod N$

Relations with RSA

C-DRSA + E-DRSA $\Leftrightarrow$ RSA

Indeed:

$$a^e \xrightarrow{C-DRSA} a^e, (a+1)^e \xrightarrow{E-DRSA} a$$

And clearly,

RSA $\Longrightarrow$ *-DRSA
C-DRSA, E-DRSA $\Longrightarrow$ D-DRSA

Difficulty of the Problems

E-DRSA = related-messages attacks [CFPR96]

E-DRSA can be solved in $\mathcal{O}(e \log^2 e)$

Practical for small exponents
Impractical as soon as e is greater than 2^{60}.

Corollary: for a small exponent e (or even any fixed one)
C-DRSA is as hard as RSA

This is also the best known attack against D-DRSA.

Intractability Assumptions

C-DRSA Assumption

C-DRSA is intractable for large enough RSA moduli

D-DRSA Assumption

D-DRSA is intractable as soon as the exponent e
is greater than 2^{60}, for large enough RSA moduli

The New Scheme

Initialization
$N = pq$ $d = e^{-1} \bmod \phi(N)$
Encryption: $m \rightarrow (A, B)$
$k \in_R \mathbb{Z}_N^\star$ $A = k^e \bmod N$ $B = (k+1)^e \times m \bmod N$
Decryption: $(A, B) \rightarrow m$
$k = A^d \bmod N$ $m = B/(k+1)^e \bmod N$

Security

OW-CPA $\Leftrightarrow$ C-DRSA

Ind-CPA $\Leftrightarrow$ D-DRSA

However, Chosen-Ciphertext Attacks can break both One-Wayness and Semantic Security (indeed, this scheme is easily malleable).

Because of the D-DRSA, one has to use a large exponent e.

First Variant

Initialization

$N = pq$

$d = e^{-1} \bmod \phi(N)$

h, hash function

Encryption: $m \rightarrow (A, B, H)$

$k \in_R \mathbb{Z}_N^\star$

$A = k^e \bmod N$

$B = (k+1)^e \times m \bmod N$

$H = h(m, k)$

Decryption: $(A, B, H) \rightarrow m$

$k = A^d \bmod N$

$m = B/(k+1)^e \bmod N$

$H \stackrel{?}{=} h(m, k)$

Security

In the Random Oracle Model

OW-CPA $\Leftrightarrow$ C-DRSA

Ind-CCA $\Leftrightarrow$ D-DRSA

Therefore, one has to use a large exponent e.

Second Variant

Initialization
$N = pq$ $d = e^{-1} \bmod \phi(N)$ g, h, hash functions
Encryption: $m \rightarrow (A, B, H)$
$k \in_R \mathbb{Z}_N^\star$ $A = k^e \bmod N$ $B = g((k+1)^e \bmod N) \oplus m$ $H = h(m, k)$
Decryption: $(A, B, H) \rightarrow m$
$k = A^d \bmod N$ $m = B \oplus g((k+1)^e \bmod N)$ $H \stackrel{?}{=} h(m, k)$

Security

In the Random Oracle Model

Ind-CCA $\Leftrightarrow$ C-DRSA

Therefore, one can use a small exponent e
which leads to both efficiency and security:

Ind-CCA $\Leftrightarrow$ RSA

Efficiency

Schemes	El Gamal	OAEP	DRSA	DRSA v2
	512	1024	1024	1024
Security				
One-Wayness	DH	RSA	C-DRSA	RSA
Ind-CPA	DDH	RSA	D-DRSA	RSA
Ind-CCA	–	RSA	–	RSA
Size (in bits)				
Plaintext	511	448	1024	1024
Ciphertext	1024	1024	2048	2208
Expansion	2	2.3	2	2.2
Encryption				
Workload/kB	6144	311	1112	280
Decryption				
Workload/kB	3072	7022	4184	3352

Conclusion

- DRSA: a new family of Problems
  - a Computational one (mostly equivalent to RSA)
  - a Decisional one
- DRSA: a new family of Cryptosystems
  - Ind-CPA (w.r.t. D-DRSA) in the standard model
  - Ind-CCA (w.r.t. RSA) in the random oracle model

$$\Rightarrow \begin{cases} \text{as secure as OAEP} \\ \text{more efficient than OAEP} \end{cases}$$