Review: Dan Bogdanov, IND-CCA2 secure cryptosystems

Aleksei Ivanov

1st November 2005

1 Short overview

The survey gives a general overview of IND-CCA2 secure cryptosystems. Related concepts are exlained also in general manner. General impression is very good. This survey should point in the right direction those who want to learn more about IND-CCA2 secure systems and see what as been done tis far.

2 General remarks

The survey is wellstructured. I as logically separated sections and subsections. Definitions are introduced right after introductio. This makes it easier to read the paper.

3 Detailed comments

In section 4 there is no hint as to how the system may be IND-CCA2 secure.

In section 7.2 there is a misuse of formulae:

- mod p should be separated from its parameters
- there should be space beween "with" and "C_1