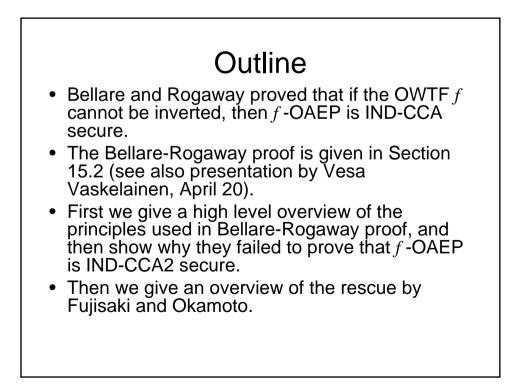
Rescue of RSA-OAEP

T-79.5502 4.5.2006



Bellare-Rogaway proof (1)

<u>Claim</u>: Let *f* be OWTF. If *f* cannot be inverted without knowledge of the private key, then *f*-OAEP is secure in IND-CCA model.

We prove this by proving:

<u>Claim</u>: If no PPT adversary has any non-negligible advantage in inverting the OWTF *f* then no PPT IND-CCA attacker *A* on *f*-OAEP has nonnegligible advantage.



• See Figure 15.3.

- *A* is an algorithm which runs IND-CCA attack. It may have some advantage guessing the bit *b*, when it is given the encryption of m_b . BUT: If the oracle returns a random ciphertext to *A* then *A* has no advantage.¹⁾ This holds if the oracle is in all aspects decent, that is, cannot be distinguished from an encryption oracle.
- *S* makes use of *A* by acting as an encryption oracle to *A*. *S* also acts as a random oracle to *A*.

¹⁾ We have used this principle before, see e.g. the lecture by Sven Laur, p.24.

Bellare-Rogaway proof (3)

- Let *A* be a PPT IND-CCA attacker on *f*-OAEP. We assume that no attacker can invert *f*.
- In particular, we assume that S cannot invert f.
- Still, *S* can accurately act as a decryption oracle to *A* in *A*'s cryptanalysis training courses. This is because if *A* wants to submit a valid ciphertext then it must query a random oracle and its queries go to *S*.

Bellare-Rogaway proof (4)

- First *S* is given $c^* = f(x)$, and *S* cannot invert *f*.
- Now *A* runs its CCA game using *S* as its decryption and random oracle.
- After the "find" stage, A submits m_0 and m_1 to S.
- S flips the coin to get bit b. Of course, S could now encrypt m_b and send the ciphertext to A. But we do not know how S could make use of such information. Instead, S send c* to A.
- With overwhelming probability we are now in a world where *c** is idependent of *m_b*. In such a world *A* has no advantage.
- With only a negligble probability we are in a world where *c** is related to *m_b*, or that *A* in some other way can detect that *S* is not an accurate oracle.
- We conclude that A has no advantage in its IND-CCA game.

Why Bellare-Rogaway proof did not achieve IND-CCA2

• The statement:

"With only a negligble probability we are in a world where c^* is related to m_b , or that A in some other way can detect that S is not an accurate oracle"

may not hold if A is allowed to make queries at the "guess" stage, after A has received the challenge ciphertext c^* .

RSA-OAEP is IND-CCA2 secure Moreover, it is shown in 15.2.3.3 that unless *A* queries *S* a value *s** such that *f*⁻¹(*c**) = *s** || *t*, we are in a world where *A* has no advantage. Problems arise only if *A* happens to submit *s** to *S*. Fujisaki and Okamoto showed: If in the guess stage *A* submits *s** such that *f*⁻¹(*c**) = *s** || *t*, where *f* is the encryption function of RSA, then *S* can find also *t*, that is, invert *f*.