Rescue of RSA-OAEP

T-79.5502

4.5.2006

Outline

- Bellare and Rogaway proved that if the OWTF f cannot be inverted, then f-OAEP is IND-CCA secure.
- The Bellare-Rogaway proof is given in Section 15.2 (see also presentation by Vesa Vaskelainen, April 20).
- First we give a high level overview of the principles used in Bellare-Rogaway proof, and then show why they failed to prove that f-OAEP is IND-CCA2 secure.
- Then we give an overview of the rescue by Fujisaki and Okamoto.

Bellare-Rogaway proof (1)

Claim: 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:

Claim: If no PPT adversary has any non-negligible advantage in inverting the OWTF f then no PPT IND-CCA attacker $\mathcal{A}$ on f-OAEP has non-negligible advantage.

Bellare-Rogaway proof (2)

- See Figure 15.3.
- $\mathcal{A}$ 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 $\mathcal{A}$ then $\mathcal{A}$ has no advantage.[1)] This holds if the oracle is in all aspects decent, that is, cannot be distinguished from an encryption oracle.
- $\mathcal{S}$ makes use of $\mathcal{A}$ by acting as an encryption oracle to $\mathcal{A}$. $\mathcal{S}$ also acts as a random oracle to $\mathcal{A}$.

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

Bellare-Rogaway proof (3)

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

Bellare-Rogaway proof (4)

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

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

RSA-OAEP is IND-CCA2 secure

- Moreover, it is shown in 15.2.3.3 that unless $\mathcal{A}$ queries $\mathcal{S}$ a value s^* such that $f^{-1}(c^*) = s^* \| t$, we are in a world where $\mathcal{A}$ has no advantage. Problems arise only if $\mathcal{A}$ happens to submit s^* to $\mathcal{S}$.
- Fujisaki and Okamoto showed:

If in the guess stage $\mathcal{A}$ submits s^* such that $f^{-1}(c^*) = s^* \| t$, where f is the encryption function of RSA, then $\mathcal{S}$ can find also t, that is, invert f .