CCA-Security

Cryptography and Protocols
Andrei Bulatov

CCA Security (take 1)

- Let (K,E,D) be a symmetric encryption scheme and (T,ε) a superpolynomial pair. Consider the following game:
  (1) Alice and Bob choose a shared k at random from $\{0,1\}^n$
  (2) Eve gets access to black boxes $E_k(\cdot)$ and $D_k(\cdot)$
  (3) Eve chooses P_1 and P_2
  (4) Alice chooses i ∈ {1,2} at random and gives Eve $C = E_k(P_i)$
  (5) Eve gets more access to black boxes $E_k(\cdot)$ and $D_k(\cdot)$
  (6) Eve outputs j ∈ {1,2}

Eve wins if j = i.

Scheme (K,E,D) is (T,ε)-CCA-secure if for any Eve of time complexity at most T Pr[Eve wins] < 1/2 + ε

CCA Security (fix)

- Change (5) to:
  (5') Eve gets access to black boxes $E_k(\cdot)$ and $D'_k(\cdot)$, where

$$D'_k(C') = \begin{cases} D_k(C'), & \text{if } C' \neq C \\ \perp, & \text{if } C' = C \end{cases}$$

Construction of a CCA-Secure Scheme

- Let (Sign, Ver) be a CMA-secure MAC and (K’,E’,D’) a CPA-secure scheme. Define (K,E,D) as follows

K: keys k, k’ selected uniformly at random from $\{0,1\}^n$

E: compute $C = E'_k(P)$, $t = \text{Sign}_{k'}(C)$, and send (C,t)

D: Upon receiving (C,t), first verify that $\text{Ver}_{k'}(C,t) = 1$
if not, abort (output $\perp$).
If check passes compute $D'_k(C)$

Security

- A MAC (Sign, Ver) satisfies the unique signatures property if for any message there at most one tag that certifies it.

  More precisely: $\text{Ver}_k(P,t)=1$ if and only if $t=\text{Sign}_k(P)$

- **Theorem**.

  Let (K,E,D) be the encryption scheme constructed as on the previous slide from a CPA-secure SES (K',E',D') and a CMA-secure MAC (Sign,Ver) that satisfies the unique signatures property. Then (K,E,D) is CCA-secure.

Security: Proof

- Idea of the proof

  Eve is allowed to make encryption and decryption queries

  Since (K',E',D') is CPA-secure, encryption queries alone don't help

  Since (Sign,Ver) is a CMA-secure scheme it is unlikely that Eve receives something different from $\perp$ to her decryption queries. Thus they are useless

- More details.

  Suppose there is Eve of bounded complexity that breaks (K,E,D).

  We construct Eve' that breaks (K',E',D')

Security: Proof (cntd)

- Eve' uses Eve and Alice, and simulates Bob:
  - choose key k'
  - whenever Eve asks for an encryption of P compute $C = E'_k(P)$ $t = \text{Sign}_{k'}(C)$ and send (C,t) to Eve. Record the query.
  - if Eve asks for decryption of what was previously computed return P
  - if Eve asks for decryption of (C,t) that was not previously computed, check if $\text{Ver}_{k'}(C,t) = 1$. If not return $\perp$. If yes, abort communication. Eve' fails to simulate Bob.
  - when Eve comes up with a challenge P_1, P_2 pass it on to Alice to obtain $C = E'_k(P_i)$. Give Eve (C,t), where $t = \text{Sign}_{k'}(C)$
  - when Eve outputs a guess j, output j