Public key crypto (quick intro)
Provable cryptography

Slides from Bart Preneel and Phil Rogaway
CPA

support(\mathcal{M}) only has strings of one length

\[ \Pi = (K,E,D) \]

\[
\text{Adv}_{\Pi}^{\text{sem}}(A) = \Pr \left[ K \leftarrow^S K; (f, M) \leftarrow^S A^{E(K, \cdot)}(); M \leftarrow^S M; C \leftarrow^S E_K(M): \right. \right.
\]
\[
A^{E(K, \cdot)}(C, f) = f(M) \left. \right] -
\]
\[
\Pr \left[ K \leftarrow^S K; (f, M) \leftarrow^S A^{E(K, \cdot)}(); M, M' \leftarrow^S M; C \leftarrow^S E_K(M'): \right. \right.
\]
\[
A^{E(K, \cdot)}(C, f) = f(M) \left. \right] \]
\( \Pi = (K, E, D) \)

\[
\text{Adv}^{\text{ind}}_{\Pi}(A) = \Pr \left[ K \leftarrow^{\$} K : A^{E(K, \cdot)} = 1 \right] - \Pr \left[ K \leftarrow^{\$} K : A^{E(K, 0 | \cdot |)} = 1 \right]
\]
\[ \text{Adv}^{\text{ind}}_{\Pi} (A) = \Pr \left[ K \xleftarrow{\$} K: A^{E(K, \cdot)} = 1 \right] - \Pr \left[ K \xleftarrow{\$} K: A^{E(K, \text{clen}(\cdot))} = 1 \right] \]
Consider a weak form of semantic security: can’t recover the key:

\[ \text{Adv}^{01}_\Pi(A) = 2 \Pr[b \leftarrow \{0,1\}; K \leftarrow \mathcal{K}; C \leftarrow E_K(b): A(C) = b] - 1 \]

Assume A does well at breaking \( \Pi \) in the 01-sense.
Construct B that does well at breaking \( \Pi \) in the ind-sense.
Def of $B^f$

Compute $C \leftarrow f(1)$

Run $A(C)$

When $A$ halts, outputting $b$

return $b$

$\text{Adv}_{\Pi}^\text{ind}(B) = \text{Pr}[B^{E(K,\cdot)} = 1] - \text{Pr}[B^{E(K, 0\mid \cdot)} = 1]$

$= \text{Pr}[K \leftarrow K; C \leftarrow E_K(1): A(C) = 1] - \text{Pr}[K \leftarrow K; C \leftarrow E_K(0): A(C) = 1]$

$= \text{Pr}[K \leftarrow K; C \leftarrow E_K(1): A(C) = 1] - (1 - \text{Pr}[K \leftarrow K; C \leftarrow E_K(0): A(C) = 0])$

$= \text{Pr}[K \leftarrow K; C \leftarrow E_K(1): A(C) = 1] + \text{Pr}[K \leftarrow K; C \leftarrow E_K(0): A(C) = 0] - 1$

$= 2 (\text{Pr}[K \leftarrow K; C \leftarrow E_K(1): A(C) = 1](0.5) + \text{Pr}[K \leftarrow K; C \leftarrow E_K(0): A(C) = 0](0.5)) - 1$

$= 2 (\text{Pr}[A \text{ returns } b \mid b=1] \text{ Pr}[b=1] + \text{Pr}[A \text{ returns } b \mid b=0] \text{ Pr}[b=0]) - 1$

$= 2 \text{ Pr}[A \text{ returns } b] - 1$

$= \text{Adv}_{\Pi}^{01}(A)$
$\text{ind}^\$ \Rightarrow \text{ind}$
Let $A$ be an ind-adversary—think of $\delta = \text{Adv}_{\Pi}^{\text{ind}}(A)$ as large.
Construct $B$ that breaks $\Pi$ in the $\text{ind}^\$-$sense$. 

\[ E_K(\cdot) \quad \geq \delta/2 \]
\[ \text{clen}(\cdot) \quad \geq \delta/2 \]

Case 1: Set $B = A$.
\[ \text{Adv}_{\Pi}^{\text{ind}^\$}(B) \geq \delta/2 \]

Case 2: Adv $B_f$ behaves as follows:
Run $A$
When $A$ asks its oracle $x$,
Ask $f(0|x|$) and return it to $A$.
When $A$ outputs a bit $b$,
return $1-b$
\[
\text{Adv}_{\Pi}^\text{ind$^\$} (t,q) \leq 2 \text{Adv}_{\Pi}^\text{ind} (t+\text{tiny}, \mu) \\
\text{tiny} = O(\mu)
\]

Suppose \( \exists \) an adv A that runs in time \( t \) and asks queries totaling \( \mu \) bits and breaks \( \Pi \) in the ind-sense with advantage \( \delta \).

Then \( \exists \) an adv B that runs in time \( t + O(\mu) \) and asks queries totaling \( \mu \) bits and breaks \( \Pi \) in the ind$^\$-sense with advantage \( \geq \delta/2 \).
\[ M_1 \oplus \text{CBC-zero} \quad M_2 \oplus \text{CBC-ctr} \quad M_3 \oplus \text{CBC-chain} \]

\[ \overline{K} \]

\[ C_1 \quad \overline{K} \quad C_2 \quad \overline{K} \quad C_3 \]

\[ \text{CBC-encctr} \quad \text{CBC-rand} \]
CBC-zero (IV = 0)  
Ask 0^n → C_1  
Ask 1^n → C_2  
if C_1 = C_2 then return 0 else return 1

CBC-ctr (IV_i = i)  
Ask 0^n → C_1  
Ask 0^{n-1} 1 → C_2  
if C_1 = C_2 then return 1 else return 0

CBC-chain (IV_i = last block of ciphertext)  
Ask 0^n → IV_1 C_1  
Ask C_1 → IV_2 C_2  
Ask C_2 → IV_3 C_3  
if C_2 = C_3 then return 1 else return 0
\( \oplus \)

\( \oplus \)

\( \oplus \)

\( K \)

\( K \)

\( K \)

\( M_1 \)

\( M_2 \)

\( M_3 \)

\( C_1 \)

\( C_2 \)

\( C_3 \)

CTR-ctr

CBC-rand
Proof outline (from Goldwasser and Bellare, chapter 6)

- We know that one-time-pad is secure
- Replace block-cipher with random function (R)
  - $R(i++) = \text{one-time-pad}$
- Shannon proved that “idealized” counter mode give any attacker zero advantage
- Construct difference between ideal and actual protocol ($\text{indS}$)
- Assume adversary $A$ can distinguish ideal and actual protocol
  - Prove that adversary $B$ could use $A$ to distinguish the block cipher from PRF
- Therefore, assuming any $B$ should have low advantage (strong cipher), then
  - Any $A$ therefore has a low advantage
Claim: CTR-rand is secure if its block cipher is a good PRP: Let A be an adv attacking CTR[E]. Construct B that attacks E.

Adversary $B^f$ behaves as follows:

Run A.
When A asks its oracle to encrypt $M=M_1 \cdots M_m$
\[ \text{ctr} \leftarrow \{0,1\} \]
compute $\text{pad} = f(\text{ctr}) f(\text{ctr}+1) \cdots f(\text{ctr}+m-1)$
return to A (ctr, pad$\oplus M$)
When A halts, outputting a bit b,
return b
\[ \text{Adv}^\text{prp}(B) = \text{Pr}[B^E_K = 1] - \text{Pr}[B^\pi = 1] \]
\[ \geq \text{Pr}[B^E_K = 1] - \text{Pr}[B^\rho = 1] - \frac{\sigma^2}{2^{n+1}} \quad \text{(switching lemma)} \]
\[ = \text{Pr}[A^\text{CTR}[E_K] = 1] - \text{Pr}[A^\text{CTR}[\rho] = 1] - \frac{\sigma^2}{2^{n+1}} \]

Let \( C \) be the event of a collision in the inputs to the blockcipher

\[ = \text{Pr}[A^\text{CTR}[E_K] = 1] - \text{Pr}[A^\text{CTR}[\rho] = 1 | C] \quad \text{Pr}[C] \]
\[ - \text{Pr}[A^\text{CTR}[E_K] = 1 | C] \quad \text{Pr}[C] - \frac{\sigma^2}{2^{n+1}} \]
\[ = \text{Pr}[A^\text{CTR}[E_K] = 1] - \text{Pr}[A^\|$ = 1] (1 - \text{Pr}[C]) \]
\[ - \text{Pr}[A^\text{CTR}[E_K] = 1 | C] \quad \text{Pr}[C] - \frac{\sigma^2}{2^{n+1}} \]
\[ = \text{Pr}[A^\text{CTR}[E_K] = 1] - \text{Pr}[A^\$ = 1] + \text{Pr}[C] \quad \text{Pr}[A^\$=1] \]
\[ - \text{Pr}[A^\text{CTR}[E_K] = 1 | C] \quad \text{Pr}[C] - \frac{\sigma^2}{2^{n+1}} \]
\[ \geq \text{Pr}[A^\text{CTR}[E_K] = 1] - \text{Pr}[A^\$ = 1] - \text{Pr}[C] - \frac{\sigma^2}{2^{n+1}} \]
\[ = \text{Adv}^{\text{ind}_E} - \text{Pr}[C] - \frac{\sigma^2}{2^{n+1}} \]

The problem is now an information theoretic one. Claim \( \text{Pr}[C] \leq \frac{\sigma^2}{2^{n+1}} \) (see next slide). We then have

\[ \geq \text{Adv}^{\text{ind}_E} - \frac{\sigma^2}{2^{n}} \]
Adversary wants to create a collision. Best way to do this is to toss one ball at a time. 

\[ \operatorname{Pr}[C] \leq \frac{1}{N} + \frac{2}{N} + \ldots + \frac{(\sigma-1)}{N} \leq \frac{\sigma^2}{2N} \]
Th. Let $E : \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$.
Let $A$ attack CBC[$E$]. Assume $A$ runs in time $t_A$ and
asks $\sigma$ total blocks and achieves advantage $\delta_A = \text{Adv}^{\text{ind}\$}_{\text{CBC}[E]}(A)$.

Then an adv $B$ that attacks $E$ and runs in time at most $t_B$
and asks at most $q_B$ queries and achieves advantage at
least $\delta_B = \text{Adv}^{\text{prp}}_E(B)$ where
\[
\begin{align*}
t_B &= t_A + O(\sigma) \\
q_B &= \sigma \\
\delta_B &= \delta_A - \sigma^2 / 2^n
\end{align*}
\]
Def of $B^f$

Run A
When A asks its oracle $M=M_1\cdots M_m$
  Choose $IV \leftarrow C_0 \leftarrow \$ \{0,1\}^n$
  for $i \leftarrow 1$ to $m$ do $C_i \leftarrow f (C_{i-1} \oplus M_i)$
  return to A (IV, C₁⋯Cₘ)
When A outputs a bit, $b$,
  return $b$
\[
\text{Adv}_{E}^{\text{prp}}(B) = \Pr[B^{\text{EK}} = 1] - \Pr[B^{\pi} = 1]
\]
\[
\text{Adv}_{\text{CBC}[E]}^{\text{ind$}}(A) = \Pr[A^{\text{CBC}[E]} = 1] - \Pr[A^{\$} = 1]
\]
\[
\text{Adv}_{\text{CBC}[E]}^{\text{ind$}}(A) - \text{Adv}_{E}^{\text{prp}}(B) = \Pr[B^{\pi} = 1] - \Pr[A^{\$} = 1]
\]
\[
= \Pr[A^{\text{CBC}[\pi]} = 1] - \Pr[A^{\$} = 1]
\]
\[
= \Pr[A^{\text{CBC}[\rho]} = 1] - \Pr[A^{\$} = 1] + \sigma^2/2^{n+1}
\]
Now a purely inf theoretic question. “Game-playing” to Show first difference at most \(\sigma^2 / 2^{n+1}\)
Authenticity

A “wins” if $C \notin \{C_1, \ldots, C_q\}$ and $D_K(C) \neq *$
“Encrypt-with-redundancy”

Attack:
Ask \(0 \, 0\) $\rightarrow$ IV C\(_1\) C\(_2\) C\(_3\)$

Forge
IV C\(_1\) C\(_2\)
MAC  “Message Auth. Code”  \( \text{MAC}_K(M) \)

\[ S^K \xrightarrow{M \cdot \text{MAC}_K(M)} R^K \]

Compute \( \sigma' = \text{MAC}_K(M) \)

Check if \( \sigma = \sigma' \)

A wins if \( \sigma = \text{MAC}_K(M) \) and \( M \notin \{M_1, \ldots, M_q\} \)

“A forgery”

\[ \text{Adv}^{\text{mac}}_\Pi (A) = \Pr[K \leftarrow \$ K : A^{\text{MAC}_K(\cdot)} \text{ forges}] \]
The CBC MAC is incorrect across msgs of varying lengths.

To forge:
Ask $0 \rightarrow \sigma_1$
Forge $(0 \sigma, \sigma)$

[BKR] Correct, with bound $3\sigma^2/2^n$ for msgs of some one fixed length.
Fixing the CBC MAC

Encrypted CBC (from RACE project). Shown provably secure (when E a PRP) by [Petrank, Rackoff]
A different fix. Provably security shown in [Black, R]
The key for the MAC is $(h,K)$

$h$ is a random element of

$$H = \{h: M \rightarrow \{0,1\}^n\}$$

Def: Family of hash functions $H = \{h: M \rightarrow \{0,1\}^n\}$ is $\varepsilon$-AU (almost universal) if for all $M, M' \in M, M \neq M'$,

$$\Pr_h [h(M) = h(M')] \leq \varepsilon$$
Unlikely for a random $h$
Eg construction

\[ M = M_m \ldots M_0 \quad |M_i| = 128 \]

\[ M(X) = X^m + M_{m-1}X^{m-1} + \ldots + M_1X + M_0 \]

All operations in GF(2^{128})

There are 2^{128} elements of \( H \), each described by a 128-bit \( R \):

\( h_R(M) = M(R) \). Can be efficiently evaluated.

Claim: \( H \) is m/2^{128}-AU where \( m \) upperbounds the number of blocks on any message \( M \) in the message space \( M \)

Proof: \( \Pr \left[ M(R) = M'(R) \right] = \Pr[\text{poly}(R) = 0] \leq m/2^{128} \) because \( \text{poly}(\cdot) \) is a nonzero polynomial of degree at most \( m \) and therefore has at most \( m \) zeros, and so that chance that a random point in the field is one of these zeros is at most \( m / \text{the size of the field} \).
The function NH used in UMAC [BHKKR]. This function is $2^{-15}$-AU. The above can be computed in just four instructions on a Pentium processor, allowing one to MAC at about 1cpb.
Authenticated Encryption via Generic Composition
(see [Bellare, Namprempre])

Encrypt-and-MAC

MAC-then-Encrypt

Encrypt-then-MAC

OK!
Authenticated Encryption via Fancy Modes
(see IAPM [J] and OCB [RBBK])