El Gamal Encryption

Slides by Prof. Jonathan Katz.
Lightly edited by me.
Dlog-based PKE
Diffie-Hellman key exchange

\begin{align*}
(G, q, g, h_1) &\leftarrow \mathcal{G}(1^n) \\
x &\leftarrow \mathbb{Z}_q \\
h_1 &= g^x \\
k &= (h_2)^x \\
m &= c_2 \cdot k^{-1}
\end{align*}

\begin{align*}
h_2 \\
c_2 &= k \cdot m
\end{align*}

\begin{align*}
y &\leftarrow \mathbb{Z}_q \\
h_2 &= g^y \\
k &= (h_1)^y
\end{align*}
El Gamal encryption

\[(G, q, g, h_1) \leftarrow \mathcal{G}(1^n)\]
\[x \leftarrow \mathbb{Z}_q\]
\[h_1 = g^x\]
\[k = (h_2)^x\]
\[m = c_2 \cdot k^{-1}\]

Public key

\[h_2, h_1^y \cdot m\]

Ciphertext

\[c_2 = k \cdot m\]

Decryption

\[y \leftarrow \mathbb{Z}_q\]
\[h_2 = g^y\]
\[k = (h_1)^y\]
El Gamal encryption

• Gen(1^n)
  – Run Gen(1^n) to obtain G, q, g. Choose uniform x ∈ ℤ_q. The public key is (G, q, g, g^x) and the private key is x

• Enc_{pk}(m), where pk = (G, q, g, h) and m ∈ G
  – Choose uniform y ∈ ℤ_q. The ciphertext is g^y, h^y·m

• Dec_{sk}(c_1, c_2), where sk = x
  – Output c_2/c_1^x = c_2 · c_1^{-x}
Security?

• If the DDH assumption is hard for $\mathcal{G}$, then the El Gamal encryption scheme is CPA-secure
  – Follows from security of Diffie-Hellman key exchange, or can be proved directly
  – Note that the discrete-logarithm assumption alone is not enough here

$\Rightarrow$ Secure for encryption of multiple messages (using the same public key)!
  – Note that sender(s) must use fresh randomness for each encryption
El Gamal in practice

• Parameters $G$, $q$, $g$ are standardized and shared

• Need to encode message as a group element
  – In some groups, there are natural ways to do this
  – In other cases, not as easy
  – Will see later a better way of resolving this issue
Chosen-ciphertext attacks?

- El Gamal encryption is *not* secure against chosen-ciphertext attacks
  - Follows from the fact that it is *malleable*

- Given ciphertext \((c_1, c_2)\), transform it to obtain the ciphertext \((c_1, c'_2) = (c_1, \alpha \cdot c_2)\) for arbitrary \(\alpha\)
  - Since \((c_1, c_2) = (g^y, h^y \cdot m)\), we have \((c_1, c'_2) = (g^y, h^y \cdot (\alpha m))\)
  - I.e., encryption of \(m\) becomes an encryption of \(\alpha m\)!
Attack!
(Assume $2 \in G \subset \mathbb{Z}_p^*$)

First bid: $m$
Second bid: $2m$