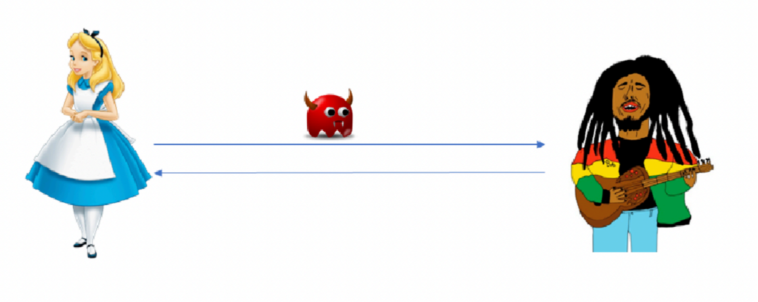
Key Exchange and the Diffie-Hellman Protocol

Michele Ciampi

Introduction to Modern Cryptography, Lecture 13

The status before 1976

- It was generally believed that secure communication could not be achieved without first sharing some secret information.
- Secure key exchange over a public untrusted channel seemed infeasible.



New Directions in Cryptography (Diffie-Hellman 1976)

- *Asymmetry* can be used to achieve secure key exchange over a public channel in the presence of eavesdroppers.
- Introduction of the notion of *public-key cryptography*.

Definition of key exchange: the setting

- Two parties, Alice and Bob, run a probabilistic protocol Π in order to generate a shared secret key.
- They begin on input 1^n and they run Π using independent random bits.
- At the end of the protocol, Alice and Bob output keys $k_A, k_B \in \{0,1\}^n$, respectively.
- **Correctness:** $k_A = k_B = k$.

Definition of key exchange: Security

Consider the following experiment for Π and adversary $\mathcal{A}$

The key-exchange experiment $\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$**:**

1. Two parties holding 1^n execute protocol Π. This results in a transcript *trans* containing all the messages sent by the parties, and a key k output by each of the parties.
2. A uniform bit $b \in \{0,1\}$ is chosen. If $b = 0$, set $\hat{k} := k$, and if $b = 1$, then choose $\hat{k} \in \{0,1\}^n$ uniformly at random.
3. The adversary $\mathcal{A}$ is given *trans* and $\hat{k}$, and outputs a bit b'.
4. The output of the experiment is 1 if $b' = b$ ($\mathcal{A}$ succeeds in guessing b), and 0 otherwise.

Definition of key exchange: Security

Definition

A key-exchange protocol Π is *secure in the presence of an eavesdropper* if for every PPT adversary $\mathcal{A}$, it holds that

$$\Pr\left[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n)\ .$$

Namely, $\mathcal{A}$ has not significantly more than a random guess probability to distinguish a real key from a key chosen uniformly at random.

The Diffie-Hellman key-exchange protocol

Let $\mathcal{G}$ be a group generation algorithm that on input 1^n outputs a description of a cyclic group $\mathbb{G}$, its order q, and a generator g.

- **Common input:** the security parameter 1^n
- **The protocol:**
  1. Alice runs $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$.
  2. Alice chooses a uniform $x \in \mathbb{Z}_q$, and computes $h_A := g^x$.
  3. Alice sends $(\mathbb{G}, q, g, h_A)$ to Bob.
  4. Bob receives $(\mathbb{G}, q, g, h_A)$. He chooses a uniform $y \in \mathbb{Z}_q$ and computes $h_B := g^y$. Bob sends h_B to Alice and outputs the key $k_B := h_A^y = (g^x)^y = g^{xy}$.
  5. Alice receives h_B and outputs the key $k_A := h_B^x = (g^y)^x = g^{xy}$.

Figure: The Diffie-Hellman key-exchange protocol.

The Diffie-Hellman key-exchange protocol

Alice		**Bob**
$x \stackrel{\$}{\leftarrow} \mathbb{Z}_q$		
$h_A := g^x$	$\xrightarrow{\mathbb{G}, q, g, h_A}$	
		$y \stackrel{\$}{\leftarrow} \mathbb{Z}_q$
	$\xleftarrow{h_B}$	$h_B := g^y$
$k_A := h_B^x$		$k_B := h_A^y$

Figure: The Diffie-Hellman key-exchange protocol.

Security of the Diffie-Hellman protocol

- The shared key g^{xy} should be indistinguishable from uniform for any adversary given g, g^x and g^y.
- The discrete-logarithm and CDH assumptions do not suffice.
- We will make use of the DDH assumption.
- We use a modified version of the key-exchange security definition, by considering the experiment $\widehat{\mathsf{KE}}^{\mathsf{eav}}_{\mathcal{A},\Pi}$, where if $b = 1$, the adversary is given $\hat{k}$ chosen uniformly from $\mathbb{G}$ instead from a uniform n-bit string.

The decisional Diffie-Hellman problem

Consider the following experiment for a group generation algorithm $\mathcal{G}$ and an adversary $\mathcal{A}$.

The DDH experiment $\mathsf{DDH}_{\mathcal{A},\mathcal{G}}(n)$**:**

1. Run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$.
2. Choose uniform $x, y, z \in \mathbb{Z}_q$.

Definition

We say that *the DDH problem is hard relative to* $\mathcal{G}$*, if for every PPT adversary* $\mathcal{A}$*, it holds that*

$$\left| \Pr\left[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^z) = 1\right] - \Pr\left[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1\right] \right| \leq$$

$\leq \mathsf{negl}(n)$, where in each case the probabilities are taken over the experiment $\mathsf{DDH}_{\mathcal{A},\mathcal{G}}(n)$.

Security of the Diffie-Hellman protocol

Theorem

If the DDH problem is hard relative to $\mathcal{G}$, then the Diffie-Hellman key-exchange protocol is secure in the presence of an eavesdropper.

Proof. In the experiment $\widehat{\mathsf{KE}}^{\mathsf{eav}}_{\mathcal{A},\Pi}$, the adversary $\mathcal{A}$ receives $(\mathbb{G}, q, g, h_A = g^x, h_B = g^y, \hat{k})$, where $(\mathbb{G}, q, g, g^x, g^y)$ is the protocol transcript and $\hat{k}$ is either the actual key g^{xy} (if $b = 0$) or a uniform group element (if $b = 1$).

Distinguishing between these two cases is exactly equivalent to solving the DDH problem!

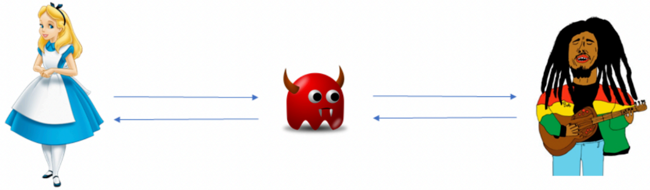
Security of the Diffie-Hellman protocol

$$
\begin{aligned}
&\Pr\left[\widehat{\mathsf{KE}}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)=1\right]=\\
=&\Pr\left[\widehat{\mathsf{KE}}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)=1\wedge(b=0)\right]+\Pr\left[\widehat{\mathsf{KE}}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)=1\wedge(b=1)\right]=\\
=&\frac{1}{2}\cdot\Pr\left[\widehat{\mathsf{KE}}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)=1\middle|b=0\right]+\frac{1}{2}\cdot\Pr\left[\widehat{\mathsf{KE}}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)=1\middle|b=1\right]=\\
=&\frac{1}{2}\cdot\Pr\left[\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^{xy})=0\right]+\frac{1}{2}\cdot\Pr\left[\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^z)=1\right]=\\
=&\frac{1}{2}\Big(1-\Pr\left[\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^{xy})=1\right]\Big)+\\
&\qquad+\frac{1}{2}\cdot\Pr\left[\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^z)=1\right]=\\
=&\frac{1}{2}+\frac{1}{2}\Big(\Pr\left[\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^z)=1\right]-\Pr\left[\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^{xy})=1\right]\Big)\\
\leq&\frac{1}{2}+\frac{1}{2}\Big|\Pr\left[\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^z)=1\right]-\Pr\left[\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^{xy})=1\right]\Big|\\
\leq&\frac{1}{2}+\frac{1}{2}\cdot\mathsf{negl}(n),\quad\text{by the hardness of the DDH problem.}
\end{aligned}
$$

□

Active attacks

- Eavesdropping is not the only possible attack.
- The adversary may send messages of its own to one or both of the parties.
- *Man-in-the-middle* attacks: the adversary is intercepting and modifying messages sent from one party to the other.



Active attacks

- The Diffie-Hellman protocol is insecure against man-in-the-middle attacks.
- A man-in-the-middle adversary can act in such a way that Alice and Bob terminate the protocol with different keys k_A and k_B, both known to the adversary.
- Neither Alice nor Bob can detect that any attack was carried out.

Exercise!

End

References: Sec 10.3, Sec 10.4.