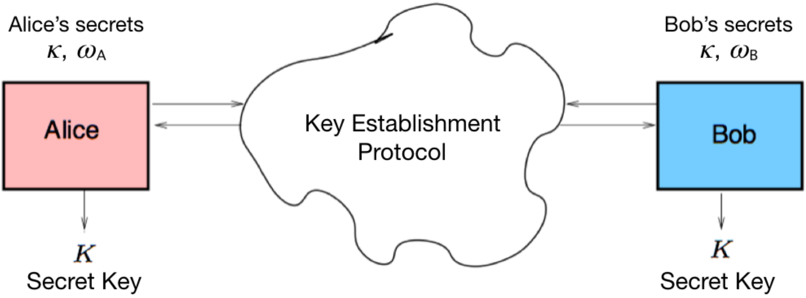
Key Establishment

Ahto Buldas

October 9, 2018

Motives

- Establishing a secret key assumes secure channel and is inconvenient
- Can we establish a key via a cryptographic protocol?



Key Establishment Protocol: Formal Definition

Goal: Having a shared key κ, Alice and Bob establish a new shared key K.

Key establishment protocol is a quadruple $(A, K_A; B, K_B)$ of functions:

◦ K_A and K_B are of type $\Omega \times \Omega \times \{0,1\}^* \to \{0,1\}^m$

◦ A and B are of type $\Omega \times \Omega \times \{0,1\}^* \to \{0,1\}^*$ and $\Omega = \{0,1\}^k$.

We assume that one bit-string is defined as STOP symbol, that indicates the end of the protocol, in case it is the output of both A and B.

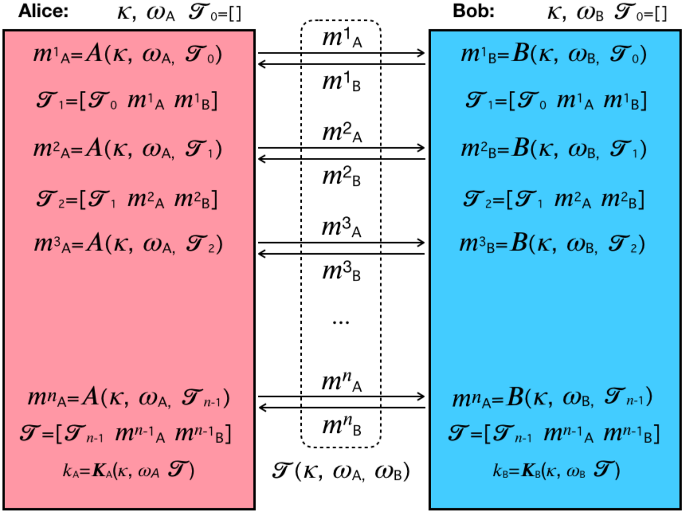
Transcript of a Protocol

Transcript $\mathcal{T}$ of the protocol is computed by the following schema:

$$\begin{aligned}\mathcal{T}_0 &= [] \\ \mathcal{T}_n &= [\mathcal{T}_{n-1}, A(\kappa, \omega_A, \mathcal{T}_{n-1}), B(\kappa, \omega_B, \mathcal{T}_{n-1})] \ .\end{aligned}$$

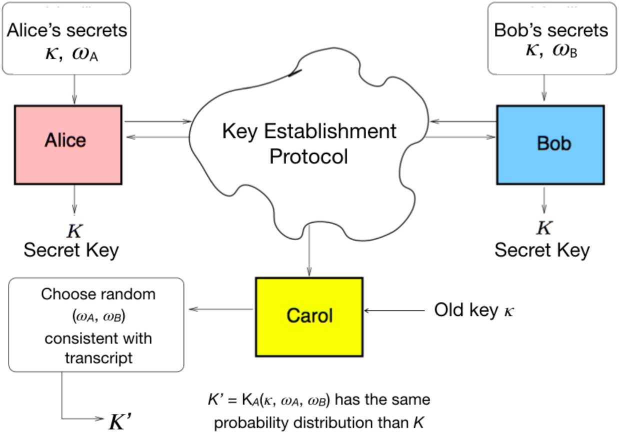
$\mathcal{T} = \mathcal{T}(\kappa, \omega_A, \omega_B) := \mathcal{T}_n(\kappa, \omega_A, \omega_B)$, where n is the smallest index such that $\mathcal{T}_n$ contains the STOP symbol, or if n was the agreed-on maximal number of rounds.

Key Establishment Protocol



Problems with Unlimited Adversaries

- No key establishment protocols are secure against unlimited adversaries!



Problems with Unlimited Adversaries

- Carol can find all possible Alice's secret keys that are consistent with the protocol flow
- Carol picks one of such keys randomly and computes her key K'
- Carol's output distribution is the same as Alice's output distribution
- Correctness of the protocol implies that with high probability, Alice's key coincides with Bob's key
- But then, with high probability, Carol's key coincides with Bob's key
- Any such a key establishment protocol is vulnerable against unlimited Carol

Key Establishment Scenario

- The keys $\kappa, \omega_A, \omega_B$ are chosen uniformly at random
- A and B generate the transcript $\mathcal{T} = \mathcal{T}(\kappa, \omega_A, \omega_B)$
- A and B compute the keys: $k_A = K_A(\kappa, \omega_A, \mathcal{T})$ and $k_B = K_B(\kappa, \omega_B, \mathcal{T})$
- C is given the old key κ
- C chooses $\omega'_A \leftarrow W_{T,A,\kappa}$ uniformly at random, where

$$W_{T,A,\kappa} = \{\omega_A \colon \exists \omega'_B : T = \mathcal{T}(\kappa, \omega_A, \omega'_B)\}$$

- C outputs $k_C = K_A(\kappa, \omega'_A, \mathcal{T})$

The *correctness* of the protocol is the probability $\gamma = \mathsf{P}[k_A = k_B]$

The *success of the adversary* C is $\delta = \mathsf{P}[k_C = k_B]$

Exchangability of Random Strings

Lemma (Exchangeability)

If $\mathcal{T}(\kappa, \omega_A, \omega_B) = T = \mathcal{T}(\kappa, \omega'_A, \omega'_B)$, *then* $\mathcal{T}(\kappa, \omega'_A, \omega_B) = T = \mathcal{T}(\kappa, \omega_A, \omega'_B)$.

Proof: By induction on the number n of rounds.

Basis $(n = 1)$: The assumption implies $A(\kappa, \omega_A, \sqcup) = T_1 = A(\kappa, \omega'_A, \sqcup)$ and $B(\kappa, \omega_B, \sqcup) = T_1 = B(\kappa, \omega'_B, \sqcup)$. Therefore:

$$\begin{aligned}
\mathcal{T}_1(\kappa, \omega'_A, \omega_B) &= [A(\kappa, \omega'_A, \sqcup)\ B(\kappa, \omega_B, \sqcup)] = [A(\kappa, \omega_A, \sqcup)\ B(\kappa, \omega_B, \sqcup)] \\
&= T_1 = [A(\kappa, \omega_A, \sqcup)\ B(\kappa, \omega'_B, \sqcup)] \\
&= \mathcal{T}_1(\kappa, \omega_A, \omega'_B)\ .
\end{aligned}$$

Step: Assume that $\mathcal{T}_{n-1}(\kappa, \omega'_A, \omega_B) = T_{n-1} = \mathcal{T}_{n-1}(\kappa, \omega_A, \omega'_B)$, where $T_{n-1} = \mathcal{T}_{n-1}(\kappa, \omega_A, \omega_B) = \mathcal{T}_{n-1}(\kappa, \omega'_A, \omega'_B)$.

Exchangability of Random Strings

By assumption, $\mathcal{T}_n(\kappa, \omega_A, \omega_B) = T_n = \mathcal{T}_n(\kappa, \omega'_A, \omega'_B)$, which implies

$$A(\kappa, \omega_A, T_1) = A(\kappa, \omega'_A, T_1) \quad \text{and} \quad B(\kappa, \omega_B, T_1) = B(\kappa, \omega'_B, T_1) \ .$$

Then by induction assumption, $\mathcal{T}_{n-1}(\kappa, \omega'_A, \omega_B) = T_{n-1}$ and hence:

$$\begin{aligned}
\mathcal{T}_n(\kappa, \omega'_A, \omega_B) &= [T_{n-1}\ A(\kappa, \omega'_A, T_{n-1})\ B(\kappa, \omega_B, T_{n-1})] \\
&= [T_{n-1}\ A(\kappa, \omega_A, T_{n-1})\ B(\kappa, \omega_B, T_{n-1})] \\
&= \mathcal{T}_n(\kappa, \omega_A, \omega_B) = T_n \ .
\end{aligned}$$

$$\begin{aligned}
\mathcal{T}_n(\kappa, \omega_A, \omega'_B) &= [T_{n-1}\ A(\kappa, \omega_A, T_{n-1})\ B(\kappa, \omega'_B, T_{n-1})] \\
&= [T_{n-1}\ A(\kappa, \omega_A, T_{n-1})\ B(\kappa, \omega_B, T_{n-1})] \\
&= \mathcal{T}_n(\kappa, \omega_A, \omega_B) = T_n \ . \quad \square
\end{aligned}$$

Rectangle Property

Consider the following three sets:

$$\begin{array}{ll} W_{T,\kappa} = \{(\omega_a, \omega_b) \colon \mathcal{T}(\kappa, \omega_a, \omega_b) = T\} & \text{all pairs } (\omega_a, \omega_b) \text{ consistent with } T \\ W_{T,A} = \{\omega_a \colon \exists \omega_b' \, \mathcal{T}(\kappa, \omega_a, \omega_b') = T\} & \text{all } \omega_a \text{ consistent with } T \\ W_{T,B} = \{\omega_b \colon \exists \omega_a' \, \mathcal{T}(\kappa, \omega_a', \omega_B) = T\} & \text{all } \omega_b \text{ consistent with } T \end{array}$$

Lemma (Rectangle Property)

$$W_{T,\kappa} = W_{T,A,\kappa} \times W_{T,B,\kappa} \ .$$

Proof: Inclusion $W_{T,\kappa} \subseteq W_{T,A,\kappa} \times W_{T,B,\kappa}$ is obvious. We prove the dual inclusion. Let $(\omega_A, \omega_B) \in W_{T,A,\kappa} \times W_{T,B,\kappa}$. By definition, there exist ω'_A and ω'_B such that $\mathcal{T}(\kappa, \omega'_A, \omega_B) = \mathcal{T}(\kappa, \omega_A, \omega'_B) = T$. By exchangeability, $\mathcal{T}(\kappa, \omega_A, \omega_B) = T$ and hence $(\omega_A, \omega_B) \in W_{T,\kappa}$. This implies the statement $W_{T,\kappa} = W_{T,A,\kappa} \times W_{T,B,\kappa}$. □

Insecurity against Unlimited Adversaries

Theorem (Success vs Correctness)

$\mathsf{P}[k_C = k_B] = \mathsf{P}[k_A = k_B]$ *in the key establishment scenario.*

Proof: It is sufficient to prove that the input distribution $\langle \omega'_A, \mathcal{T}\rangle$ of C coincides with A's input distribution $\langle \omega_A, \mathcal{T}\rangle$. Indeed, for every a and T:

$$\begin{aligned}
\mathsf{P}[\omega'_A = a, \mathcal{T} = T] &= \mathsf{P}[\mathcal{T} = T]\cdot\mathsf{P}[\omega'_A = a \mid \mathcal{T} = T] = \frac{|W_{T,\kappa}|}{|\Omega|^2}\cdot\frac{1}{|W_{T,A,\kappa}|} \\
&= \frac{|W_{T,A,\kappa}\times W_{T,B,\kappa}|}{|\Omega|^2\cdot|W_{T,A,\kappa}|} = \frac{|W_{T,A,\kappa}|\cdot|W_{T,B,\kappa}|}{|\Omega|^2\cdot|W_{T,A,\kappa}|} = \frac{|W_{T,B,\kappa}|}{|\Omega|^2}
\end{aligned}$$

$$\begin{aligned}
\mathsf{P}[\omega_A = a, \mathcal{T} = T] &= \sum_b \mathsf{P}[\omega_A = a]\,\mathsf{P}[\omega_B = b][T = \mathcal{T}(\kappa, a, b)] \\
&= \frac{1}{|\Omega|^2}\sum_b [T = \mathcal{T}(\kappa, a, b)] = \frac{|W_{T,B,\kappa}|}{|\Omega|^2}\ . \qquad \square
\end{aligned}$$

Limits of the Information-Theoretical Security Model

Key Size: The size of the encryption key is close to the size of the encrypted message.

No Key Establishment: Key establishment protocols are insecure against unlimited adversaries.

Computational Security Model

Limited adversaries: Adversary can use limited amount of computational resources:

- *Time*, i.e. the number of operations
- *Memory*, i.e. the number of bits stored during computations
- *Program Size*, i.e. the number of commands in the attacking program

If the limits are met, we say that the adversary is *efficient*

Program A $\longrightarrow$

Breakage task $\longrightarrow$

$\longrightarrow$ Result

One-Way Functions

A function $f\colon \{0,1\}^* \to \{0,1\}^*$ is *one-way* if it is:

◦ *Easy to compute*: There is a program F that uses reasonable resources and computes $f(x) \leftarrow \mathsf{F}(x)$ for all $x \in \{0,1\}^*$.

◦ *Hard to Invert*: For every efficient program A the probability

$$\mathsf{P}[x \leftarrow \{0,1\}^k, x' \leftarrow \mathsf{A}(f(x))\colon\ f(x') = f(x)]$$

is negligibly small.

Modular Exponent Function

Let p be a big prime number $\alpha \in \mathbb{Z}_p$ be the so-called *primitive element*, i.e. all powers $\alpha^1, \alpha^2, \ldots, \alpha^{p-1}$ are different modulo p.

Then the *modular exponent function*:

$$f_{\alpha,p}(x) = \alpha^x \mod p$$

is believed to be one-way.

Diffie-Hellman Key Establishment

In 1976, Whitfield Diffie and Martin Hellman proposed the following single-round key establishment protocol based on modular exponentiation:

- A and B choose $\omega_A \leftarrow \{1, \ldots, p-1\}$ and $\omega_B \leftarrow \{1, \ldots, p-1\}$
- A computes $y_A = \alpha^{\omega_A} \bmod p$ and sends $m_A^1 = y_A$ to B
- B computes $y_B = \alpha^{\omega_B} \bmod p$ and sends $m_B^1 = y_B$ to A
- A computes $k_A = y_B^{\omega_A} \bmod p = \alpha^{\omega_A \omega_B} \bmod p$
- B computes $k_B = y_A^{\omega_B} \bmod p = \alpha^{\omega_B \omega_A} \bmod p = k_A$

Man in the Middle Attack

Diffie-Hellman key establishment is not secure against *active adversaries*

Carol can send Bob her own α^{ω_C} instead of Alice's α^{ω_A}

Carol can send Alice her own α^{ω_C} instead of Bob's α^{ω_B}