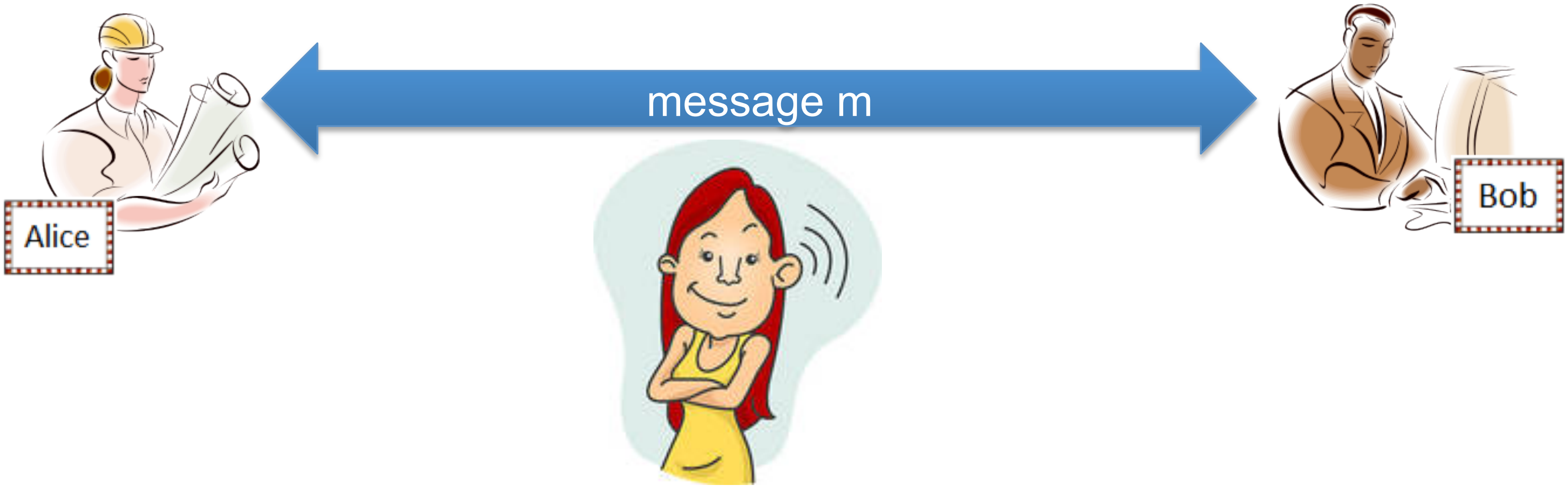
II. Digital signatures



1. **Did Bob send message m, or was it Eve?**

2. **Did Eve modify the message m, that was sent by Bob?**

Digital signatures

Digital signatures

- are equivalents of handwritten signatures
- guarantee authenticity and integrity of documents
- also guarantee non-repudiation

Digital signatures

Definition 2.1 A digital signature scheme Π is a triple of probabilistic polynomial time algorithms (ppts) $(\text{Gen}, \text{Sign}, \text{Vrfy})$, where

1. $\text{Gen}(1^n)$ outputs a key pair (pk, sk) with $|pk|, |sk| \geq n$.
2. Sign takes as input a secret key sk and a message $m \in \{0,1\}^*$ and outputs a signature σ, $\sigma \leftarrow \text{Sign}_{sk}(m)$.
3. Vrfy takes as input a public key pk, a message $m \in \{0,1\}^*$, and a signature σ. It ouputs $b \in \{0,1\}$, $1 \triangleq$ valid, $0 \triangleq$ invalid. Vrfy deterministic, $b := \text{Vrfy}_{pk}(m, \sigma)$.

For every key pair (pk, sk) and message m:
$\text{Vrfy}_{pk}(m, \text{Sign}_{sk}(m)) = 1$.

Digital signatures

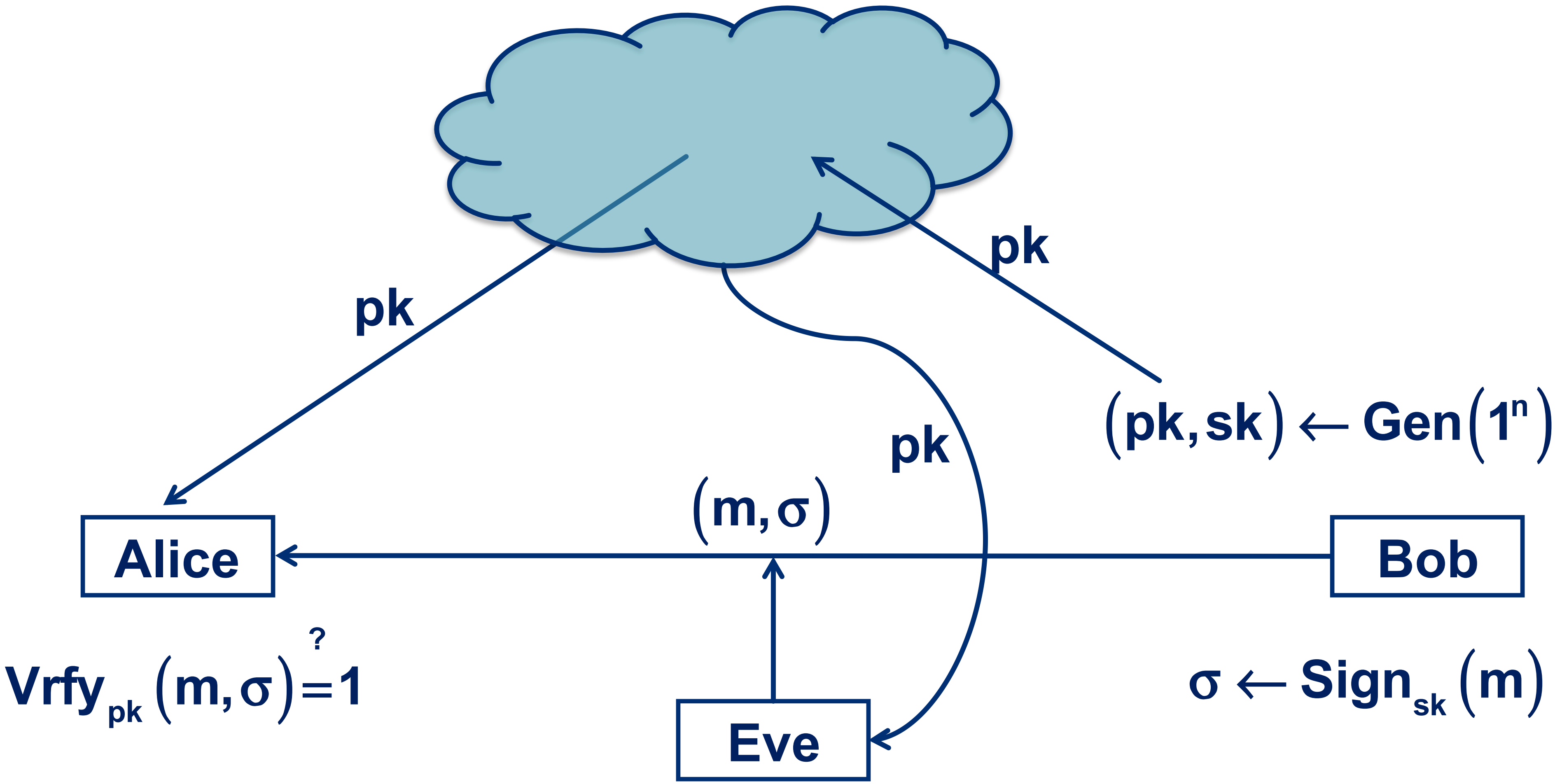
Definition 2.1 A digital signatur scheme Π is a triple of probabilistic polynomial time algorithms (ppts) $(\mathrm{Gen}, \mathrm{Sign}, \mathrm{Vrfy})$, where

1. $\mathrm{Gen}(1^n)$ outputs a key pair (pk, sk) with $|pk| = |sk| = n$.
2. Sign takes as input a secret key sk and a message $m \in \{0,1\}^*$ and outputs a signature σ, $\sigma \leftarrow \mathrm{Sign}_{sk}(m)$.
3. Vrfy takes as input a public key pk, a message $m \in \{0,1\}^*$, and a signature σ. It ouputs $b \in \{0,1\}$, $1 \triangleq$ valid, $0 \triangleq$ invalid. Vrfy determinitic, $b := \mathrm{Vrfy}_{pk}(m, \sigma)$.

For every key pair (pk, sk) and message m: $\mathrm{Vrfy}_{pk}(m, \mathrm{Sign}_{sk}(m)) = 1$.

If $(\mathrm{Gen}, \mathrm{Sign}, \mathrm{Vrfy})$ is such that for every (pk,sk) output by $\mathrm{Gen}(1^n)$, algorithm Sign_{sk} is only defined for $m \in \{0,1\}^{l(n)}$, then we say that (Gen, Sign, Vrfy) is a signature scheme for messages of length l(n).

Digital signatures



Security of digital signatures

- An adversary should not be able to compute the signature for an arbitrary message even though he knows the public key of correct signer.
- This should remain true, even if the adversary can get signatures for messages of his choice.
- But the adversary must compute the signature for a new message to be successful.
- Restrict adversaries to efficient ones.
- But adversaries should succeed only with tiny probability.

The forging game

Signature forging game $\text{Sig-forge}_{A,\Pi}(n)$

1. $(pk, sk) \leftarrow \text{Gen}(1^n)$.
2. A is given $1^n, pk$ and oracle access to $\text{Sign}_{sk}(\cdot)$. It outputs pair (m, σ). $\mathcal{Q} := $ set of queries made by A to $\text{Sign}_{sk}(\cdot)$.
3. Output of experiment is 1, if and only if (1) $\text{Vrfy}_{pk}(m, \sigma) = 1$, and (2) $m \notin \mathcal{Q}$.

Definition 2.2 Π is called existentially unforgeable under an adaptive chosen-message attack, or secure, if for every ppt adversary A there is a negligible function $\mu : \mathbb{N} \to \mathbb{R}^+$ such that

$$\Pr\left[\text{Sig-forge}_{A,\Pi}(n) = 1\right] = \mu(n).$$

Oracle access

Algorithm D has oracle access to function $f: U \rightarrow R$, if

1. D can write elements $x \in U$ into special memory cells,
2. in one step receives function value $f(x)$.

Notation Often write $D^{f(\cdot)}$ to denote that algorithm D has oracle access to $f(\cdot)$.

Negligible functions

Definition 2.3 A function $\mu : \mathbb{N} \to \mathbb{R}^+$ is called negligible, if

$$\forall c \in \mathbb{N}\ \exists n_0 \in \mathbb{N}\ \forall n \geq n_0\ \mu(n) \leq 1/n^c.$$

RSA signatures - prerequisites

$\mathbb{Z}_N$:= ring of integers modulo N

$\mathbb{Z}_N^*$:= $\{a \in \mathbb{Z}_N : \gcd(a,N) = 1\}$

$\phi(N)$:= $|\mathbb{Z}_N^*|$

$$\gcd(a,m) = 1 \quad \Rightarrow \quad \exists\, u,v \in \mathbb{Z}\; u \cdot a + v \cdot m = 1 \;\; \text{(EEA)}$$

$$\Rightarrow \quad u \cdot a = 1 \bmod m$$

$$\Rightarrow \quad u = a^{-1} \bmod m$$

$$N = \prod_{i=1}^{K} p_i^{e_i} \quad \Rightarrow \quad \phi(N) = \prod_{i=1}^{K} \left(p_i^{e_i} - p_i^{e_i - 1}\right) = N \cdot \prod_{i=1}^{K} \left(1 - 1/p_i\right) \cdot$$

RSA signatures

$\mathrm{Gen}(1^n)$: choose 2 random primes $p,q \in [2^{n-1}, 2^n - 1]$,

$N := p \cdot q, e \leftarrow \mathbb{Z}^*_{\phi(N)}, d := e^{-1} \bmod \phi(N)$,

$pk := (N,e), sk := (N,d)$.

$\mathrm{Sign}_{sk}(m)$ $m \in \{0,1\}^{2n-2}$ interpreted as element in $\mathbb{Z}_N$,

$\sigma := m^d \bmod N$.

$\mathrm{Vrfy}_{pk}(m,\sigma)$ output 1, if and only if $\sigma^e = m \bmod N$.

RSA signatures - correctness

For special case $m \in \mathbb{Z}_N^*$ based on

Lemma 2.4 Let $N \in \mathbb{N}$ and $m \in \mathbb{Z}_N^*$, then $m^{\phi(N)} = 1 \bmod N$.

RSA signatures - efficiency

Prime generation

1. choose $p \leftarrow \left[2^{n-1}, 2^n - 1\right]$.
2. Test whether p is prime, if so output p, otherwise go back to 1.

Efficiency based on

1. In $\left[2^{n-1}, 2^n - 1\right]$ many primes exist (prime number theorem).
2. Efficient primality test exist (Miller-Rabin, AKS)

RSA signatures - efficiency

Exponent generation

1. choose $e \leftarrow \mathbb{Z}_{\phi(N)}$.
2. Test whether $\gcd(e, \phi(N)) = 1$, if so compute d with $e \cdot d = 1 \bmod \phi(N)$, otherwise go back to 1.

Efficiency based on

1. In $\mathbb{Z}_M$ many elements relatively prime to M exist.
2. Can check efficiently whether $a,b \in \mathbb{Z}$ are relatively prime using Eucledean algorithm.

RSA signatures - efficiency

Efficiency of Sign and Vrfy based on

1. Arithmetic in $\mathbb{Z}_N$ can be done efficiently.
2. Exponentiation requires few arithmetic operations using Square-and-Multiply.

RSA signatures - forgeries

existential forgeries

- $\text{Sign}_{sk}(0) = 0$
- $\text{Sign}_{sk}(1) = 1$
- $\text{Sign}_{sk}(-1) = -1$

selective forgery of $\text{Sign}_{sk}(m)$

- query signature oracle with input $\hat{m} := 2^e m \bmod N$ and obtain $\hat{\sigma}$.
- compute $\sigma = 2^{-1}\hat{\sigma} \bmod N$.

General problem of public-key cryptography

Secret key sk must not be efficiently computable from public key pk!

General problem for RSA

Given (N,e), element $d \in \mathbb{Z}^*_{\phi(N)}$ with $e \cdot d = 1 \bmod \phi(N)$ must not be efficiently computable.

Theorem 2.5 Given e,d,N, $N = p \cdot q$ for primes p,q, and with $e \cdot d = 1 \bmod \varphi(N)$, then the primes p,q can be computed in time polynomial in $\log(N)$.

Status of factoring problem

Two factoring algorithms

– Number field sieve

running time $\exp\left(\log(N)^{1/3} \cdot \log\log(N)^{2/3}\right)$

– Elliptic curve method

running time $\exp\left(\log(p)^{1/2} \cdot \log\log(p)^{1/2}\right)$,

where p smallest prime factor

Existence of secure signatures

Theorem 2.6 **Secure digital signature schemes exist if and only if one-way functions exist.**

- **We will not prove this theorem entirely.**
- **But present the most important steps.**
- **The difficult direction is the construction of secure signatures from one-way functions.**

Inverting game

$f:\{0,1\}^* \to \{0,1\}^*$, A a probabilistic polynomial time algorithm

Inverting game $\text{Invert}_{A,f}(n)$

1. $x \leftarrow \{0,1\}^n, y := f(x)$.
2. A given input 1^n and y, outputs x'.
3. Output of game is 1, if $f(x') = y$, otherwise output is 0.

Write $\text{Invert}_{A,f}(n) = 1$, if output is 1. Say A has succeded or A has won.

Definition of one-way function

Definition 2.7 $f:\{0,1\}^* \to \{0,1\}^*$ called one-way, if

1. there is a ppt M_f with $M_f(x)=f(x)$ for all $x \in \{0,1\}^*$
2. for every probabilistic polynomial time algorithm A there is a negligible function $\mu:\mathbb{N}\to\mathbb{R}^+$ such that $\Pr\left[\text{Invert}_{A,f}(n)=1\right]=\mu(n)$.

Notation $\Pr_{x\leftarrow\{0,1\}^n}\left[A(f(x))\in f^{-1}(f(x))\right]=\mu(n)$

Candidate

1. $$f_{mult}: \{0,1\}^* \rightarrow \{0,1\}^*$$
$$x \mapsto (x_1 \cdot x_2, |x_1|, |x_2|),$$

where $|x_1| = \lfloor |x|/2 \rfloor, |x_2| = \lceil |x|/2 \rceil$, and identify bit strings and integers via binary representations.

Idea Multiplication easy, factoring hard