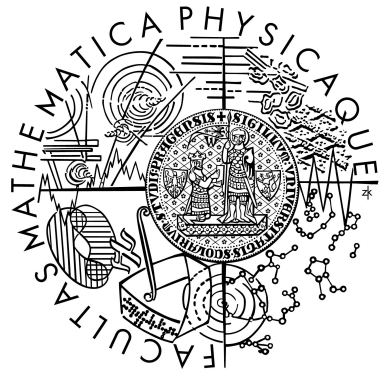
Attacking RSA

Barbora Hudcová
Igor Eržiak



FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

25.11.2016

Contents

Introduction

Low Exponent RSA with Related Messages

Wiener's Attack

Coppersmith's Attack

Introduction

Definition (RSA cryptosystem)

Let $N = pq$ be the product of two primes. Let e, d be two integers satisfying

$$ed \equiv 1 \pmod{\phi(N)}$$

where $\phi(N) = (p-1)(q-1)$.

Introduction

Definition (RSA cryptosystem)

Let $N = pq$ be the product of two primes. Let e, d be two integers satisfying

$$ed \equiv 1 \pmod{\phi(N)}$$

where $\phi(N) = (p-1)(q-1)$.

N ... RSA modulus

Introduction

Definition (RSA cryptosystem)

Let $N = pq$ be the product of two primes. Let e, d be two integers satisfying

$$ed \equiv 1 \pmod{\phi(N)}$$

where $\phi(N) = (p-1)(q-1)$.

N ... RSA modulus

e ... encryption exponent

Introduction

Definition (RSA cryptosystem)

Let $N = pq$ be the product of two primes. Let e, d be two integers satisfying

$$ed \equiv 1 \pmod{\phi(N)}$$

where $\phi(N) = (p-1)(q-1)$.

- N ... RSA modulus
- e ... encryption exponent
- d ... decryption exponent

Introduction

Definition (RSA cryptosystem)

Let $N = pq$ be the product of two primes. Let e, d be two integers satisfying

$$ed \equiv 1 \pmod{\phi(N)}$$

where $\phi(N) = (p-1)(q-1)$.

- N ... RSA modulus
- e ... encryption exponent
- d ... decryption exponent
- $\langle N, e \rangle$ ... public key

Introduction

Definition (RSA cryptosystem)

Let $N = pq$ be the product of two primes. Let e, d be two integers satisfying

$$ed \equiv 1 \pmod{\phi(N)}$$

where $\phi(N) = (p-1)(q-1)$.

- N ... RSA modulus
- e ... encryption exponent
- d ... decryption exponent
- $\langle N, e \rangle$ ... public key
- $\langle N, d \rangle$ ... private key

Meet the Crew

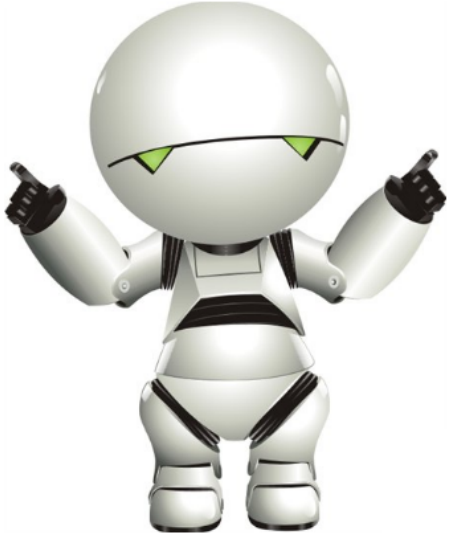
Bob

Alice

Meet the Crew

Bob

Marvin



Alice

Introduction

$\langle N, e \rangle$

$\langle N, d \rangle$

Introduction

$\langle N, e \rangle$

$M \in \mathbb{Z}_N^*$

$\langle N, d \rangle$

Introduction

$\langle N, e \rangle$

$M \in \mathbb{Z}_N^*$

$C \equiv M^e \pmod{N}$

$\langle N, d \rangle$

Introduction

$\langle N, e \rangle$

$M \in \mathbb{Z}_N^*$

$C \equiv M^e \pmod{N}$

$\langle N, d \rangle$

$C^d \pmod{N}$

Introduction

$\langle N, e \rangle$

$M \in \mathbb{Z}_N^*$

$C \equiv M^e \pmod{N}$

$\langle N, d \rangle$

$C^d \pmod{N}$

Indeed, from Euler's theorem it follows that

$$C^d \equiv M^{ed} \equiv M \pmod{N}.$$

Low Exponent RSA with Related Messages

M. Franklin

M. Reiter

Low Exponent RSA with Related Messages

M. Franklin

M. Reiter

Artist: Milan Boháček

Low Exponent RSA with Related Messages

What does Marvin know?

Low Exponent RSA with Related Messages

What does Marvin know?

- public key $\langle N, e \rangle$

Low Exponent RSA with Related Messages

What does Marvin know?

- public key $\langle N, e \rangle$
- k ciphertexts of different messages produced using the same public key $\langle N, e \rangle$

Low Exponent RSA with Related Messages

What does Marvin know?

- public key $\langle N, e \rangle$
- k ciphertexts of different messages produced using the same public key $\langle N, e \rangle$
- polynomial relation between the messages

Low Exponent RSA with Related Messages

What does Marvin know?

- public key $\langle N, e \rangle$
- k ciphertexts of different messages produced using the same public key $\langle N, e \rangle$
- polynomial relation between the messages

What is Marvin's goal?

Low Exponent RSA with Related Messages

What does Marvin know?

- public key $\langle N, e \rangle$
- k ciphertexts of different messages produced using the same public key $\langle N, e \rangle$
- polynomial relation between the messages

What is Marvin's goal?

- to recover the plaintext messages

Two messages with affine relation

$m_1, m_2 \in \mathbb{Z}_N^*, \quad m_2 = \alpha m_1 + \beta, \quad \alpha, \beta \in \mathbb{Z}_N^*$

$$\begin{aligned} c_1 &\equiv m_1^e \pmod N \\ c_2 \equiv m_2^e &\equiv (\alpha m_1 + \beta)^e \pmod N \end{aligned}$$

$$\begin{aligned} m_1^e - c_1 &\equiv 0 \pmod N \\ (\alpha m_1 + \beta)^e - c_2 &\equiv 0 \pmod N \end{aligned}$$

Let z denote the unknown message m_1:

$$\begin{aligned} z^e - c_1 &\equiv 0 \pmod N \\ (\alpha z + \beta)^e - c_2 &\equiv 0 \pmod N \end{aligned}$$

Applying Euclidean algorithm should yield the linear polynomial $z - m_1$.

$$z - m_1 = \gcd\left(z^e - c_1, (\alpha m_1 + \beta)^e - c_2\right) \quad \in \mathbb{Z}_N[x]$$

Two messages with polynomial relation

We have $p \in \mathbb{Z}_N[x], \quad m_2 = p(m_1), \quad \deg(p) = \delta.$

$$z^e - c_1 \equiv 0 \pmod{N}$$
$$(p(z))^e - c_2 \equiv 0 \pmod{N}$$

Euclidean algorithm should yield $z - m_1$.

$$z - m_1 = \gcd\left(z^e - c_1, (p(z))^e - c_2\right) \quad \in \mathbb{Z}_N[x]$$

Resultant

$$p(x) = p_m x^m + \ldots + p_1 x + p_0, \quad deg(p) = m$$
$$q(x) = q_n x^n + \ldots + q_1 x + q_0, \quad deg(q) = n$$

Resultant

$$p(x) = p_m x^m + \ldots + p_1 x + p_0, \quad deg(p) = m$$
$$q(x) = q_n x^n + \ldots + q_1 x + q_0, \quad deg(q) = n$$

$$Res_x(p,q) = \begin{vmatrix} p_m & 0 & 0 & \ldots & 0 & q_n & 0 & 0 & \ldots & 0 \\ p_{m-1} & p_m & 0 & \ldots & 0 & q_{n-1} & q_n & 0 & \ldots & 0 \\ p_{m-2} & p_{m-1} & p_m & \ldots & 0 & q_{n-2} & q_{n-1} & q_n & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_1 & p_2 & p_3 & \ldots & \vdots & q_1 & q_2 & q_3 & \ldots & \vdots \\ p_0 & p_1 & p_2 & \ldots & \vdots & q_0 & q_1 & q_2 & \ldots & \vdots \\ 0 & p_0 & p_1 & \ldots & \vdots & 0 & q_0 & q_1 & \ldots & \vdots \\ \vdots & \vdots & \vdots & \ddots & p_1 & \vdots & \vdots & \vdots & \ddots & q_1 \\ 0 & 0 & 0 & \ldots & p_0 & 0 & 0 & 0 & \ldots & q_0 \end{vmatrix}.$$

Resultant

$$p(x) = p_m x^m + \ldots + p_1 x + p_0, \quad deg(p) = m$$
$$q(x) = q_n x^n + \ldots + q_1 x + q_0, \quad deg(q) = n$$

$$Res_x(p,q) = \begin{vmatrix} p_m & 0 & 0 & \ldots & 0 & q_n & 0 & 0 & \ldots & 0 \\ p_{m-1} & p_m & 0 & \ldots & 0 & q_{n-1} & q_n & 0 & \ldots & 0 \\ p_{m-2} & p_{m-1} & p_m & \ldots & 0 & q_{n-2} & q_{n-1} & q_n & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_1 & p_2 & p_3 & \ldots & \vdots & q_1 & q_2 & q_3 & \ldots & \vdots \\ p_0 & p_1 & p_2 & \ldots & \vdots & q_0 & q_1 & q_2 & \ldots & \vdots \\ 0 & p_0 & p_1 & \ldots & \vdots & 0 & q_0 & q_1 & \ldots & \vdots \\ \vdots & \vdots & \vdots & \ddots & p_1 & \vdots & \vdots & \vdots & \ddots & q_1 \\ 0 & 0 & 0 & \ldots & p_0 & 0 & 0 & 0 & \ldots & q_0 \end{vmatrix}.$$

Fact: The resultant of two polynomials with coefficients in an integral domain is zero if and only if they have a common divisor of positive degree.

Implicit polynomial relation

What if m_1 and m_2 satisfy an implicit polynomial relation?

$$p(m_1, m_2) \equiv 0 \pmod{N}, \quad deg(p) = \delta$$

Then we have:

$$\begin{aligned} P_1 &= p(m_1, m_2) \equiv 0 \pmod{N} \\ P_2 &= m_1^e - c_1 \equiv 0 \pmod{N} \\ P_3 &= m_2^e - c_2 \equiv 0 \pmod{N} \end{aligned}$$

Implicit polynomial relation

$$P_1 = p(x, y) \equiv 0 \pmod{N}$$
$$P_2 = x^e - c_1 \equiv 0 \pmod{N}$$
$$P_3 = y^e - c_2 \equiv 0 \pmod{N}$$

Implicit polynomial relation

$$P_1 = p(x, y) \equiv 0 \pmod{N}$$
$$P_2 = x^e - c_1 \equiv 0 \pmod{N}$$
$$P_3 = y^e - c_2 \equiv 0 \pmod{N}$$

Resultant of $P_1(x, y)$ and $P_2(x)$ with respect to the variable x will yield a polynomial $P_4(y), \deg(P_4) \leq \delta e$.

Implicit polynomial relation

$$P_1 = p(x, y) \equiv 0 \pmod{N}$$
$$P_2 = x^e - c_1 \equiv 0 \pmod{N}$$
$$P_3 = y^e - c_2 \equiv 0 \pmod{N}$$

Resultant of $P_1(x, y)$ and $P_2(x)$ with respect to the variable x will yield a polynomial $P_4(y), \deg(P_4) \leq \delta e$.

$\gcd(P_3, P_4)$ should yield the linear polynomial $y - m_2$

Implicit polynomial relation

$$P_1 = p(x, y) \equiv 0 \pmod{N}$$
$$P_2 = x^e - c_1 \equiv 0 \pmod{N}$$
$$P_3 = y^e - c_2 \equiv 0 \pmod{N}$$

Resultant of $P_1(x, y)$ and $P_2(x)$ with respect to the variable x will yield a polynomial $P_4(y), \deg(P_4) \leq \delta e$.

$\gcd(P_3, P_4)$ should yield the linear polynomial $y - m_2$

$\gcd(P_1, P_2)$ should yield the linear polynomial $x - m_1$

Arbitrary polynomial relationship among messages

We have $m_1, m_2, \ldots, m_k$; $\quad p(m_1, \ldots, m_k) = 0$.

$$
\begin{aligned}
P_0(x_1, \ldots, x_k) = p(x_1, \ldots, x_k) &\equiv 0 \pmod{N} \\
P_1(x_1) = x_1^e - c_1 &\equiv 0 \pmod{N} \\
&\vdots \\
P_k(x_k) = x_k^e - c_k &\equiv 0 \pmod{N}
\end{aligned}
$$

Arbitrary polynomial relationship among messages

We have $m_1, m_2, \ldots, m_k$; $\quad p(m_1, \ldots, m_k) = 0$.

$$
\begin{aligned}
P_0(x_1, \ldots, x_k) = p(x_1, \ldots, x_k) &\equiv 0 \pmod{N} \\
P_1(x_1) = x_1^e - c_1 &\equiv 0 \pmod{N} \\
&\vdots \\
P_k(x_k) = x_k^e - c_k &\equiv 0 \pmod{N}
\end{aligned}
$$

$$
\begin{aligned}
Q_0(x_1, \ldots, x_k) &= P_0 \\
&\vdots \\
Q_i(x_{i+1}, \ldots, x_k) &= Res_{x_i}(Q_{i-1}, P_i) \\
&\vdots \\
Q_{k-1}(x_k)
\end{aligned}
$$

Arbitrary polynomial relationship among messages

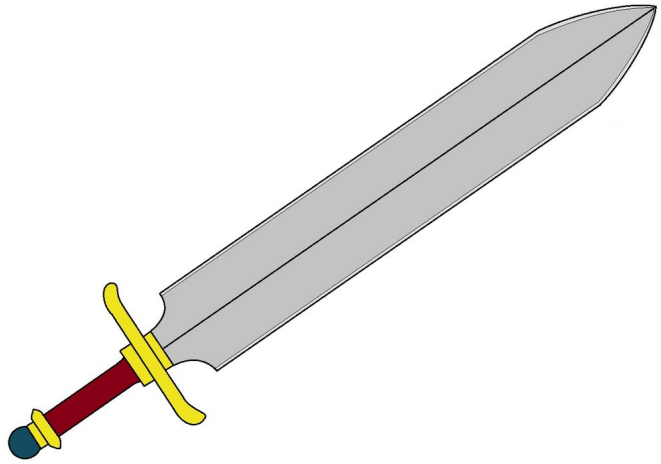
We have $m_1, m_2, \ldots, m_k$; $\quad p(m_1, \ldots, m_k) = 0$.

$$\begin{aligned} P_0(x_1, \ldots, x_k) = p(x_1, \ldots, x_k) &\equiv 0 \pmod{N} \\ P_1(x_1) = x_1^e - c_1 &\equiv 0 \pmod{N} \\ &\vdots \\ P_k(x_k) = x_k^e - c_k &\equiv 0 \pmod{N} \end{aligned}$$

$$\begin{aligned} Q_0(x_1, \ldots, x_k) &= P_0 \\ &\vdots \\ Q_i(x_{i+1}, \ldots, x_k) &= Res_{x_i}(Q_{i-1}, P_i) \\ &\vdots \\ Q_{k-1}(x_k) & \end{aligned}$$

$$\begin{aligned} \gcd\left(Q_{k-1}(x_k), P_k(x_k)\right) &= x_k - m_k \\ &\vdots \\ \gcd\left(P_i(x_i), Q_{i-1}(x_i, m_{i+1}, \ldots, m_k)\right) &= x_i - m_i \end{aligned}$$

Wiener's Attack



Wiener's Attack

Theorem (M. Wiener)

Let $N = pq$ with $q < p < 2q$. Let $d < \frac{1}{3}N^{\frac{1}{4}}$. Given a public key $\langle N, e\rangle$ with $ed \equiv 1 \pmod{\phi(N)}$, an adversary can efficiently recover d.

$$ed - k\phi(N) = 1 \quad k\phi(N) = ed - 1 \quad e < \phi(N) \implies k < d < \frac{1}{3}N^{\frac{1}{4}}$$

$$\left|\frac{e}{\phi(N)} - \frac{k}{d}\right| = \frac{1}{d\phi(N)}$$

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed - k\phi(N) + k\phi(N) - kN}{Nd}\right| =$$

$$\left|\frac{k(N - \phi(N)) - 1}{Nd}\right| \leq \left|\frac{3k\sqrt{N}}{Nd}\right| = \frac{3k}{d\sqrt{N}} \leq \frac{1}{dN^{\frac{1}{4}}} < \frac{1}{2d^2}$$

Wiener's Attack

$$\left| \frac{e}{N} - \frac{k}{d} \right| < \frac{1}{2d^2}$$

Wiener's Attack

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

$\Longrightarrow$ $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N}$ (Lemma 3)

Wiener's Attack

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

$\Longrightarrow$ $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N}$ (Lemma 3)

$\Longrightarrow$ $\frac{e}{N}$ has maximum of $\log_2 N$ convergents

Wiener's Attack

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

$\Longrightarrow$ $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N}$ (Lemma 3)

$\Longrightarrow$ $\frac{e}{N}$ has maximum of $\log_2 N$ convergents

$\Longrightarrow$ we obtain k and d

Wiener's Attack

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

$\Longrightarrow$ $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N}$ (Lemma 3)

$\Longrightarrow$ $\frac{e}{N}$ has maximum of $\log_2 N$ convergents

$\Longrightarrow$ we obtain k and d

$\Longrightarrow$ we obtain $\phi(N)$

Wiener's Attack

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

$\Longrightarrow$ $\frac{k}{d}$ is a convergent of the continued fraction expansion of $\frac{e}{N}$ (Lemma 3)

$\Longrightarrow$ $\frac{e}{N}$ has maximum of $\log_2 N$ convergents

$\Longrightarrow$ we obtain k and d

$\Longrightarrow$ we obtain $\phi(N)$

$\Longrightarrow$ we can factor N

Countermeasures

1. $\langle N, e \rangle \rightarrow \langle N, e^{'} \rangle, \quad e^{'} = e + t\phi(N)$ for some large t.
   If $e^{'} > N^{1.5}$ attack cannot be mounted.

Countermeasures

1. $\langle N, e\rangle \rightarrow \langle N, e^{'}\rangle, \quad e^{'} = e + t\phi(N)$ for some large t.
   If $e^{'} > N^{1.5}$ attack cannot be mounted.
2. CRT: choose d so that

$$d_p = d \bmod p - 1 \qquad \textit{and} \qquad d_q = d \bmod q - 1$$

   are both small.

Decryption:

$$M_p = C^{d_p} \pmod{p}$$
$$M_q = C^{d_q} \pmod{q}$$

Countermeasures

1. $\langle N, e\rangle \rightarrow \langle N, e^{'}\rangle, \quad e^{'} = e + t\phi(N)$ for some large t.
   If $e^{'} > N^{1.5}$ attack cannot be mounted.
2. CRT: choose d so that

$$d_p = d \bmod p - 1 \qquad \textit{and} \qquad d_q = d \bmod q - 1$$

   are both small.

Decryption:

$$M_p = C^{d_p} \pmod{p}$$
$$M_q = C^{d_q} \pmod{q}$$

Using CRT find $M \in \mathbb{Z}_N$ satisfying:

$$M \equiv M_p \pmod{p} \quad \& \quad M \equiv M_q \pmod{q}$$

$$M = C^d \pmod{N}$$

d_p and d_q are small but d mod $\phi(N)$ can be large.

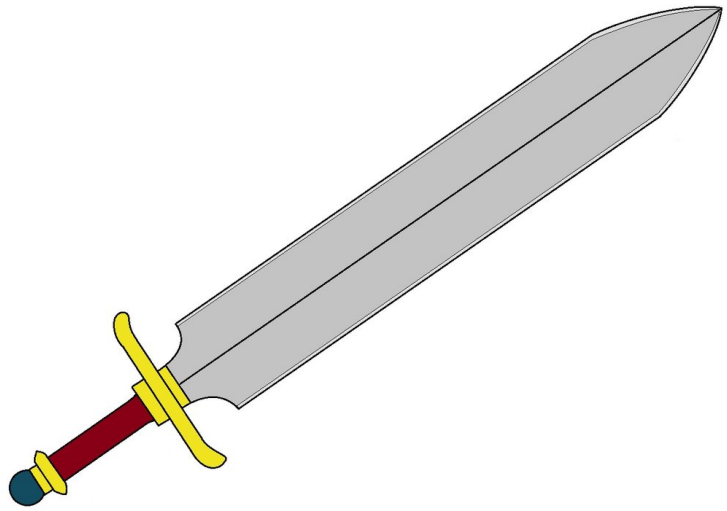
Wiener's Attack

Boneh and Durfee: $d < N^{0.292}$

Open Problem

Let $N = pq$ and $d < N^{0.5}$. If Marvin is given $\langle N, e \rangle$ with $ed \equiv 1 \pmod{\phi(N)}$ and $e < \phi(N)$, can he recover d?

Coppersmith's Attack



Theorem 5

- $N \in \mathbb{Z}$

Theorem 5

- $N \in \mathbb{Z}$
- $f \in \mathbb{Z}[x]$ is monic, $\deg(f) = \delta$

Theorem 5

- $N \in \mathbb{Z}$
- $f \in \mathbb{Z}[x]$ is monic, $\deg(f) = \delta$
- $X := N^{\frac{1}{\delta}-\epsilon}$ for some $\epsilon \geq 0$

Theorem 5

- $N \in \mathbb{Z}$
- $f \in \mathbb{Z}[x]$ is monic, $\deg(f) = \delta$
- $X := N^{\frac{1}{\delta} - \epsilon}$ for some $\epsilon \geq 0$

Then, given $\langle N, f \rangle$, Marvin can efficiently find all integers $|x_0| < X$ satisfying

$$f(x_0) \equiv 0 \pmod{N}$$

The running time is dominated by the time it takes to run the LLL algorithm on a lattice of dimension $O(w)$ with
$w = min(\frac{1}{\epsilon}, log_2(N))$.

Lemma 6

Let $h(x) \in \mathbb{Z}[x]$ be a polynomial of degree δ, and let X be a positive integer. Suppose $\|h(xX)\| < \frac{N}{\sqrt{\delta}}$. If $|x_0| < X$ satisfies $h(x_0) \equiv 0 \pmod{N}$ then $h(x_0) = 0$ holds over the integers.

Lemma 6

Let $h(x) \in \mathbb{Z}[x]$ be a polynomial of degree δ, and let X be a positive integer. Suppose $\|h(xX)\| < \frac{N}{\sqrt{\delta}}$. If $|x_0| < X$ satisfies $h(x_0) \equiv 0 \pmod{N}$ then $h(x_0) = 0$ holds over the integers.

Theorem (Cauchy-Schwarz)

For each $u_1, \ldots, u_n \in \mathbb{C}$ and $v_1, \ldots, v_n \in \mathbb{C}$:

$$\sum_{i=1}^{n} \left| u_i^T v_i \right| \leq \sum_{j=1}^{n} |u_j|^2 \sum_{k=1}^{n} |v_k|^2$$

$$f(x_0) \equiv 0 \mod N$$
$$f(x_0)^k \equiv 0 \mod N^k$$
$$g_{u,v}(x) := N^{m-v} x^u f(x)^v$$

where $0 \leq v \leq m$ and $0 \leq u$.

$$f(x_0) \equiv 0 \mod N$$
$$f(x_0)^k \equiv 0 \mod N^k$$
$$g_{u,v}(x) := N^{m-v} x^u f(x)^v$$

where $0 \leq v \leq m$ and $0 \leq u$.

$$g_{u,v}(x) := N^{m-v} x^u f(x)^v$$

$$g_{u,v}(x) := N^{m-v} x^u f(x)^v$$

GOAL Find an integer linear combination $h(x)$ of polynomials $g_{u,v}(x)$ such that $\|h(xX)\| < \frac{N^m}{\sqrt{deg(h)}}$.

$$g_{u,v}(x) := N^{m-v} x^u f(x)^v$$

GOAL Find an integer linear combination $h(x)$ of polynomials $g_{u,v}(x)$ such that $\|h(xX)\| < \frac{N^m}{\sqrt{deg(h)}}$.

How to find $h(x)$?

Lattices

Definition

Let $u_1, \ldots, u_\omega \in \mathbb{Z}^\omega$ be linearly independent vectors. A (full-rank) lattice $\mathcal{L}$ spanned by $\langle u_1, \ldots, u_\omega \rangle$ is defined as:

$$\mathcal{L} := a_1 u_1 + \cdots + a_\omega u_\omega \in \mathbb{Z}.$$

$$\det(\mathcal{L}) := \det \begin{pmatrix} - & u_1 & - \\ & \vdots & \\ - & u_\omega & - \end{pmatrix}$$

LLL Algorithm

INPUT $b_1, \ldots, b_\omega$ - basis of $\mathcal{L}$ ($\mathcal{L}$ is spanned by $\langle b_1, \ldots, b_\omega \rangle$)

OUTPUT $b'_1, \ldots, b'_\omega$ - basis of $\mathcal{L}$ satisfying:

$$\|b'_1\| \leq \|b'_2\| \leq \cdots \leq \|b'_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega}}$$

LLL Algorithm

INPUT $b_1, \ldots, b_\omega$ - basis of $\mathcal{L}$ ($\mathcal{L}$ is spanned by $\langle b_1, \ldots, b_\omega \rangle$)

OUTPUT $b'_1, \ldots, b'_\omega$ - basis of $\mathcal{L}$ satisfying:

$$\|b'_1\| \leq \|b'_2\| \leq \cdots \leq \|b'_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega}}$$

$$\|b'_1\| \leq 2^{\frac{\omega}{4}} \det(\mathcal{L})^{\frac{1}{\omega}}$$

Our case

We view polynomials $g_{u,v}(x)$ as vectors and study the lattice $\mathcal{L}$ spanned by them.
We let:

$$v = 0, \ldots, m$$

$$u = 0, \ldots, \delta - 1$$

Hence the lattice has dimension $\omega = \delta(m + 1)$.

Some big matrix called G

$g_{u,v}(x) := N^{m-v} x^u f(x)^v \qquad v = 0, \ldots, m \qquad u = 0, \ldots, \delta - 1$
$\omega = \delta(m+1)$

$$
\begin{array}{c}
 \\
g_{0,0}(xX) \\
g_{1,0}(xX) \\
g_{2,0}(xX) \\
\vdots \\
g_{\delta-1,0}(xX) \\
g_{0,1}(xX) \\
\vdots \\
g_{\delta-1,m}
\end{array}
\begin{array}{c}
\begin{array}{ccccccccc}
1 & x^1 & x^2 & \cdots & x^{\delta-1} & x^{\delta} & \cdots & x^{\delta(m+1)-1}
\end{array} \\
\begin{pmatrix}
N^m & & & & & & & \\
\vdots & N^m X & & & & & & \\
\vdots & \ddots & N^m X^2 & & & & & \\
\vdots & & \ddots & \ddots & & & & \\
\vdots & & & \ddots & N^m X^{\delta-1} & & & \\
\vdots & & & & \ddots & N^{m-1} X^{\delta} & & \\
\vdots & & & & & \ddots & \ddots & \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & X^{\delta(m+1)-1}
\end{pmatrix}
\end{array}
$$

Some big matrix called G

$g_{u,v}(x) := N^{m-v} x^u f(x)^v \qquad v = 0, \ldots, m \qquad u = 0, \ldots, \delta - 1$
$\omega = \delta(m+1)$

$$
\begin{array}{c}
 \\
g_{0,0}(xX) \\
g_{1,0}(xX) \\
g_{2,0}(xX) \\
\vdots \\
g_{\delta-1,0}(xX) \\
g_{0,1}(xX) \\
\vdots \\
g_{\delta-1,m}
\end{array}
\begin{array}{c}
\begin{array}{ccccccccc}
1 & x^1 & x^2 & \cdots & x^{\delta-1} & x^{\delta} & \cdots & x^{\delta(m+1)-1}
\end{array} \\
\begin{pmatrix}
N^m & & & & & & & \\
\vdots & N^m X & & & & & & \\
\vdots & \ddots & N^m X^2 & & & & & \\
\vdots & & \ddots & \ddots & & & & \\
\vdots & & & \ddots & N^m X^{\delta-1} & & & \\
\vdots & & & & \ddots & N^{m-1} X^{\delta} & & \\
\vdots & & & & & \ddots & \ddots & \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & X^{\delta(m+1)-1}
\end{pmatrix}
\end{array}
$$

$$det(G) = N^{\frac{1}{2}\delta m(m+1)} X^{\frac{1}{2}(\delta(m+1)-1)(\delta(m+1))} = N^{\frac{1}{2}m\omega} X^{\frac{1}{2}(\omega-1)\omega}$$

Applying the LLL algorithm on matrix the G we obtain a polynomial $h(xX) \in \mathcal{L}$:

$$\|h(xX)\| \leq 2^{\frac{\omega}{4}} \det(G)^{\frac{1}{\omega}} =$$

$$= 2^{\frac{\omega}{4}} N^{\frac{1}{2}m} X^{\frac{1}{2}(\omega-1)} \leq \frac{N^m}{\sqrt{\omega}} \ldots \text{ for large enough } m$$

Applying the LLL algorithm on matrix the G we obtain a polynomial $h(xX) \in \mathcal{L}$:

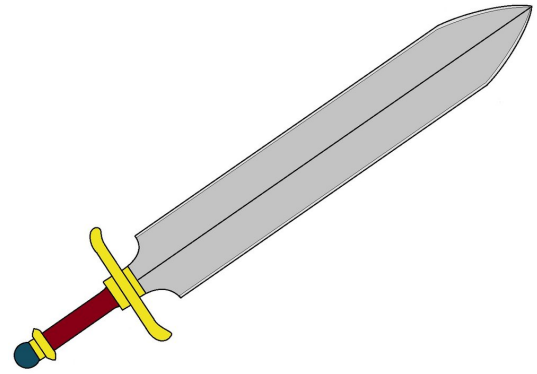
$$\|h(xX)\| \leq 2^{\frac{\omega}{4}} \det(G)^{\frac{1}{\omega}} =$$

$$= 2^{\frac{\omega}{4}} N^{\frac{1}{2}m} X^{\frac{1}{2}(\omega-1)} \leq \frac{N^m}{\sqrt{\omega}} \ldots \text{ for large enough } m$$

Let $h(x) \in \mathbb{Z}[x]$ be a polynomial of degree δ, and let X be a positive integer. Suppose $\|h(xX)\| < \frac{N}{\sqrt{\delta}}$. If $|x_0| < X$ satisfies $h(x_0) \equiv 0 \pmod{N}$ then $h(x_0) = 0$ holds over the integers.

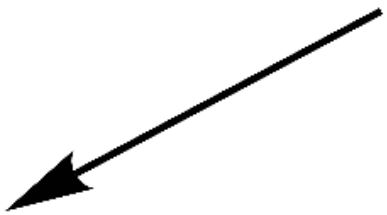
Applications of Coppersmith's Theorem

Håstad's Broadcast Attack

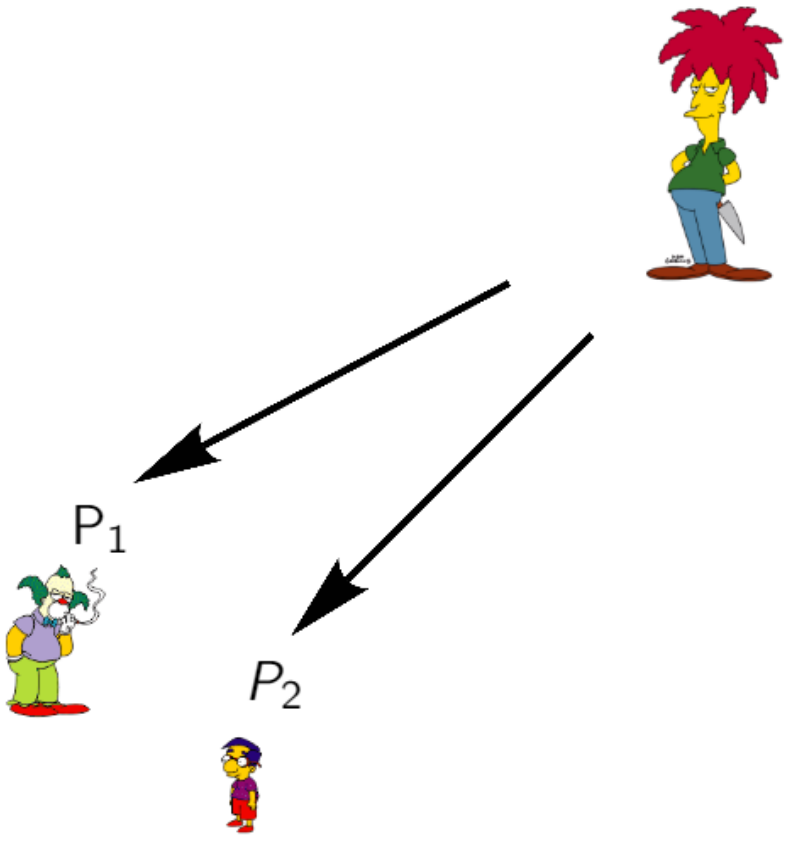


M . . . message

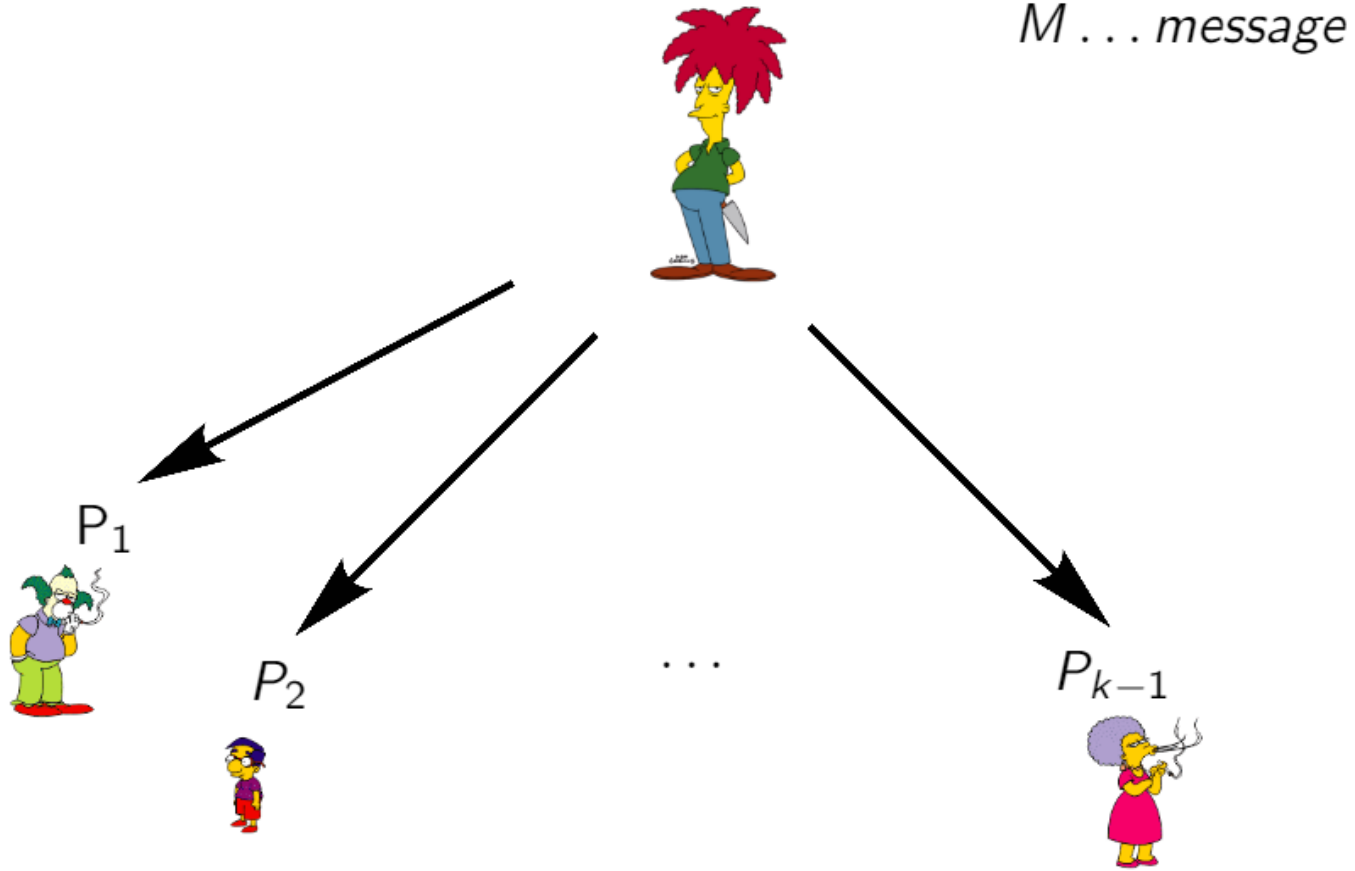
M . . . message

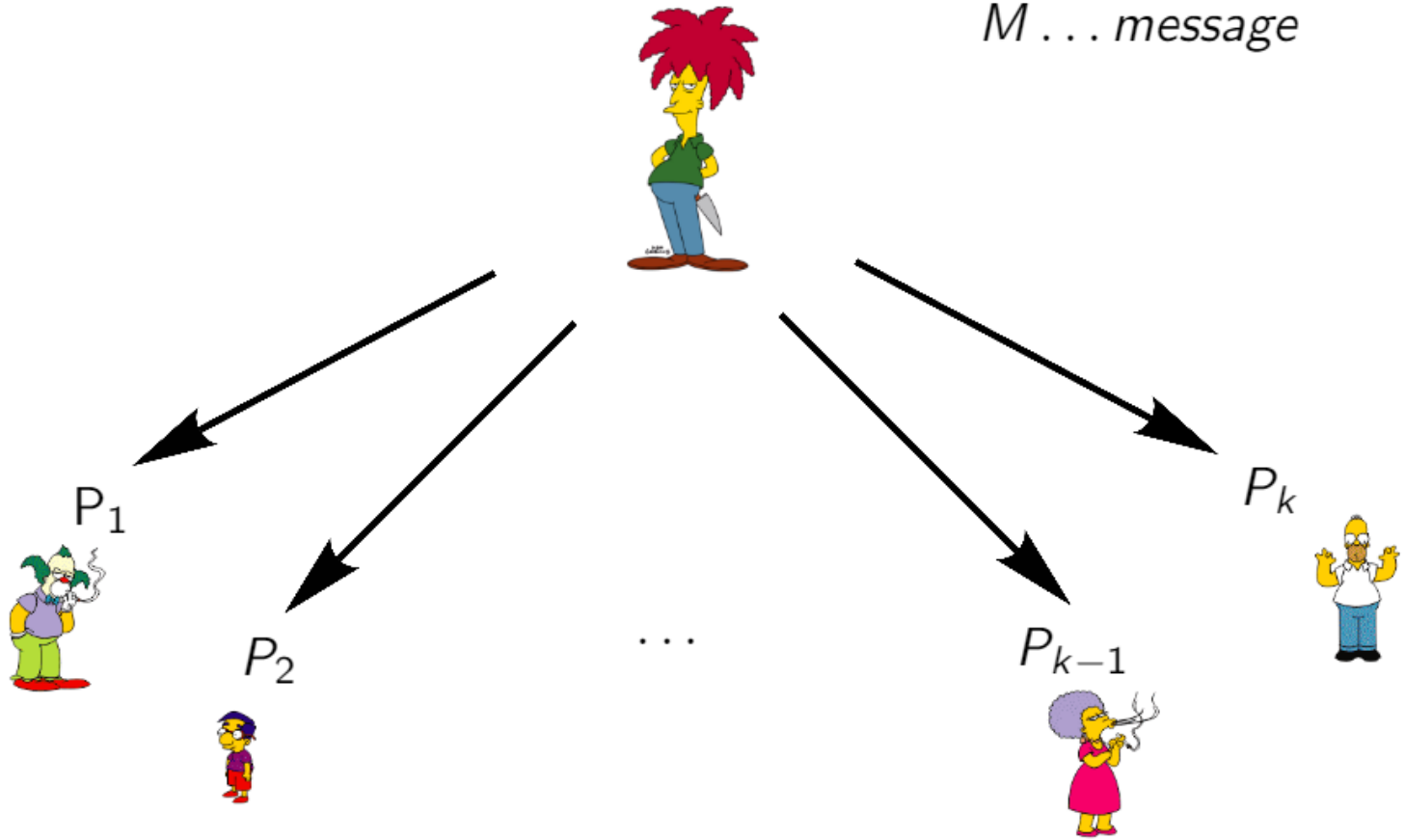


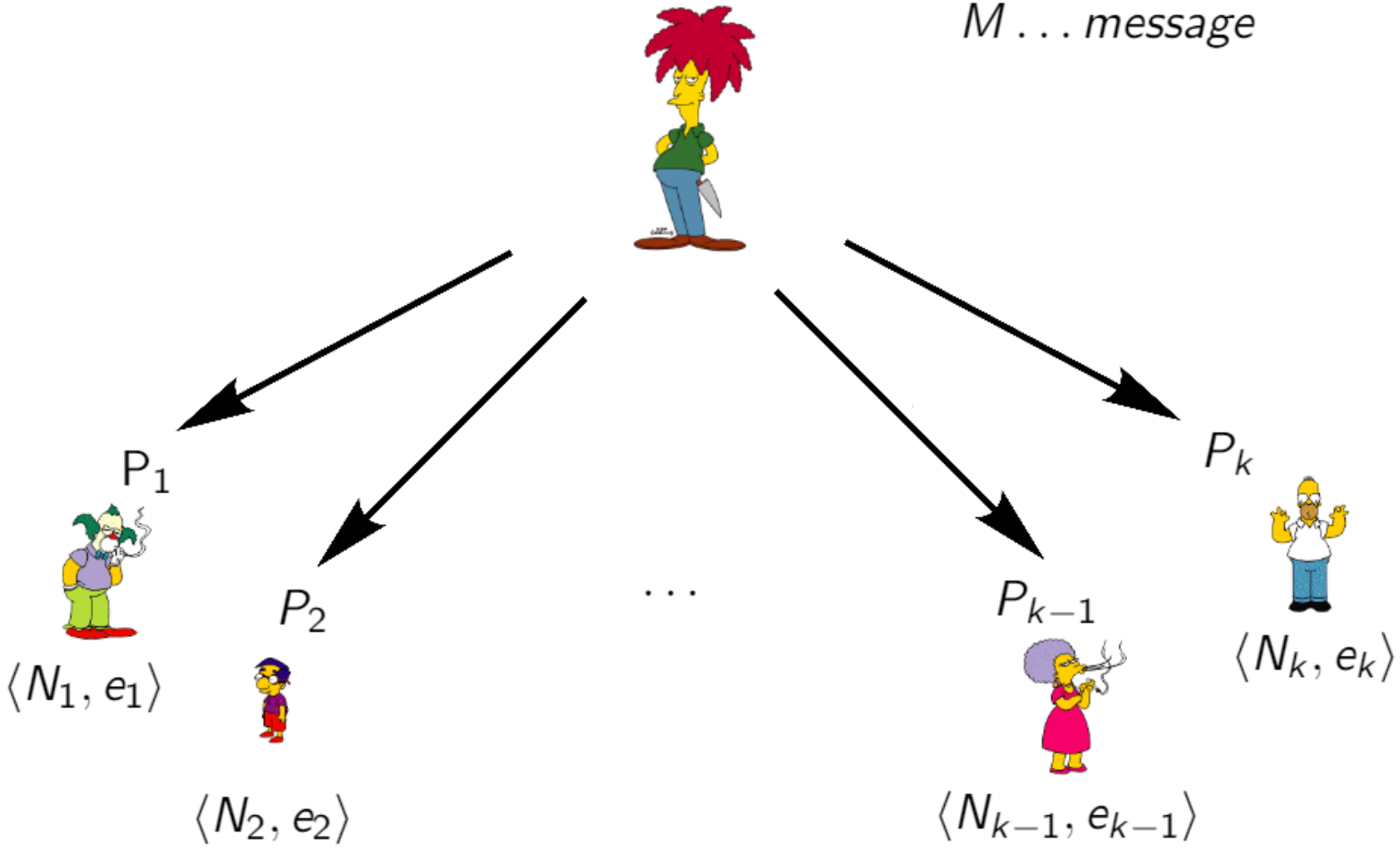
P_1

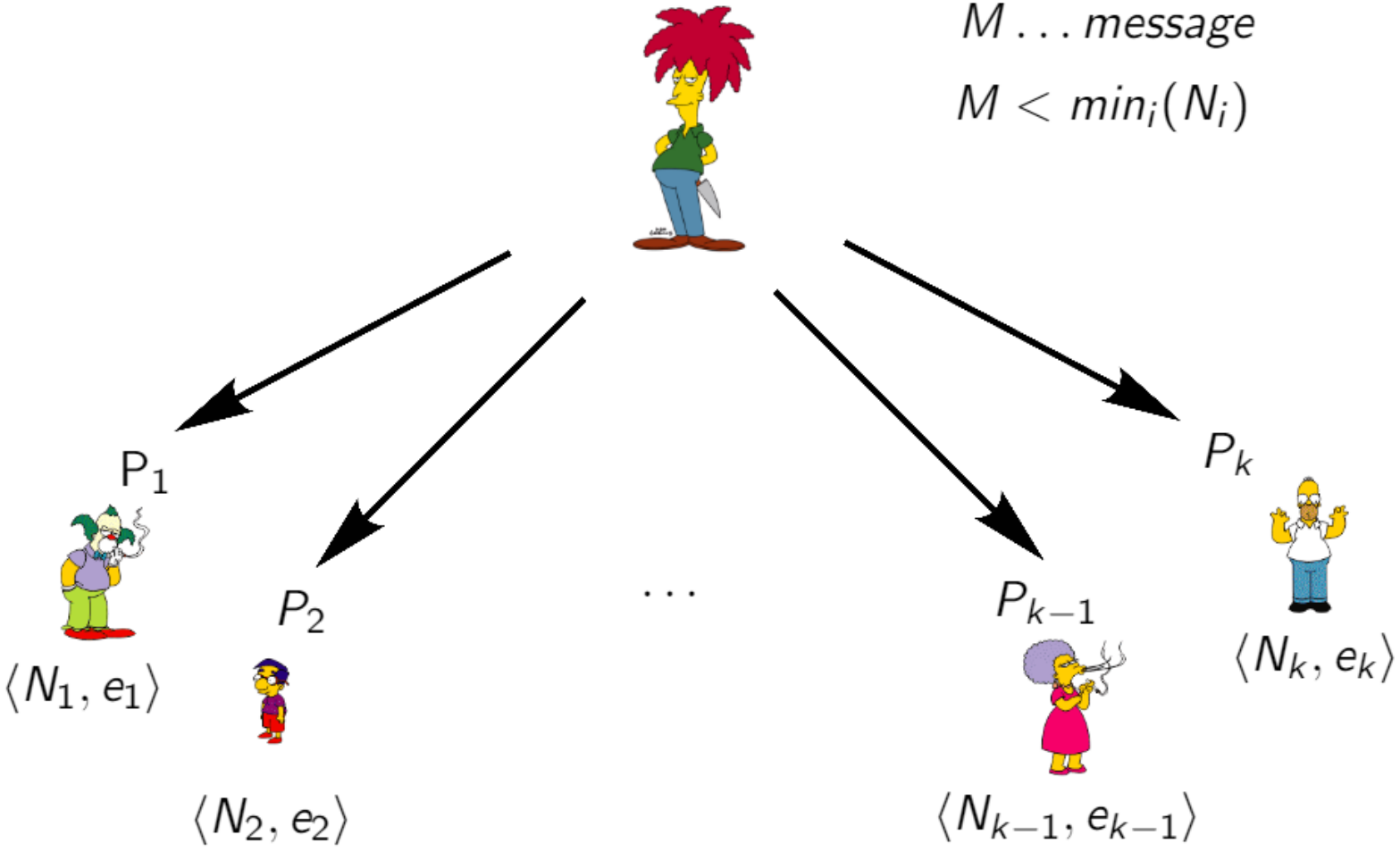


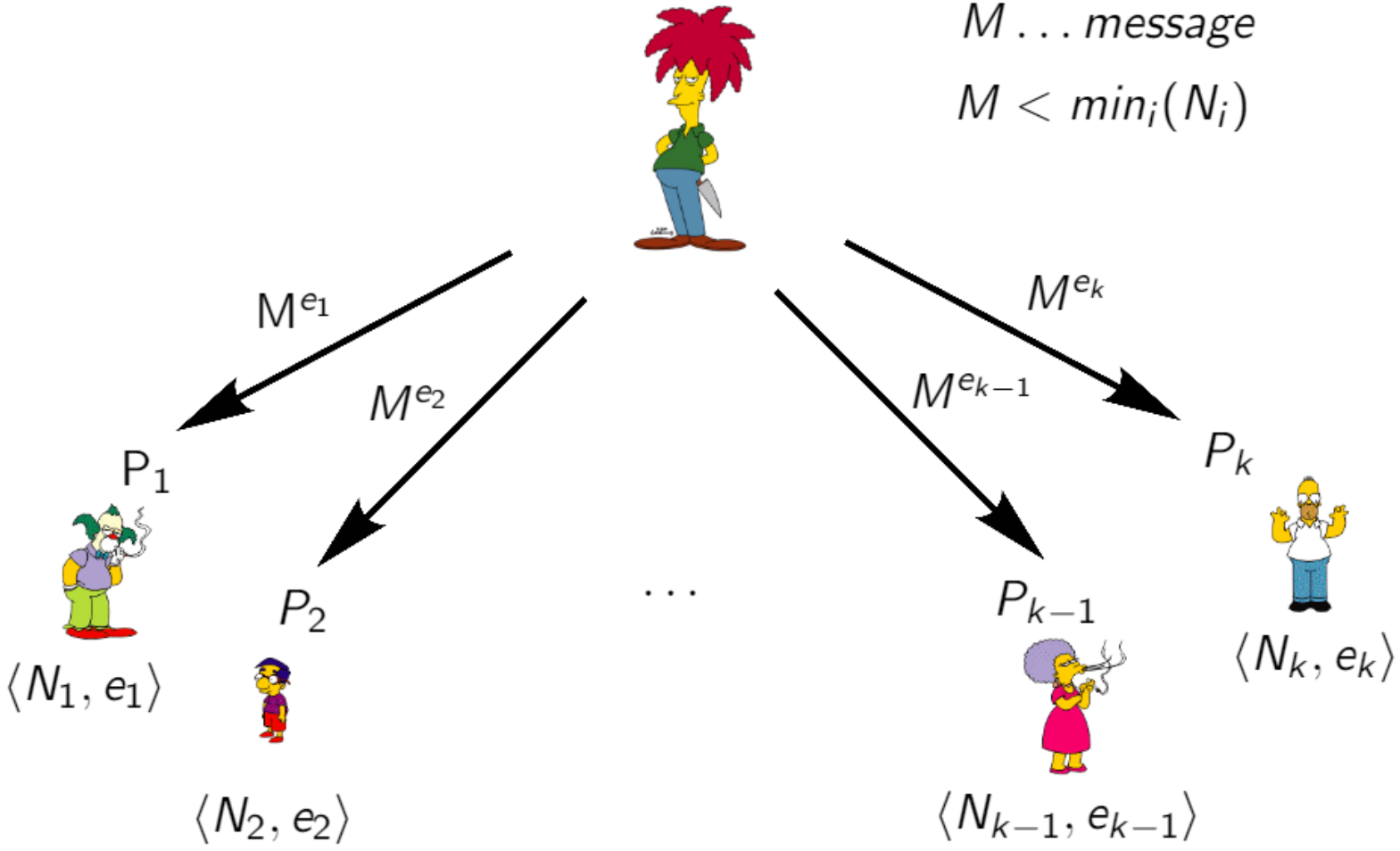
M . . . message


M . . . message
P1
P2
. . .
Pk−1


M . . . message
P1
P2
. . .
Pk−1
Pk


M . . . message
P1
P2
. . .
Pk−1
Pk
⟨N1, e1⟩
⟨N2, e2⟩
⟨Nk−1, ek−1⟩
⟨Nk, ek⟩


$M \ldots message$
$M < min_i(N_i)$
P_1
P_2
$\ldots$
P_{k-1}
P_k
$\langle N_1, e_1 \rangle$
$\langle N_2, e_2 \rangle$
$\langle N_{k-1}, e_{k-1} \rangle$
$\langle N_k, e_k \rangle$


$M \ldots message$
$M < min_i(N_i)$
M^{e_1}
M^{e_2}
$M^{e_{k-1}}$
M^{e_k}
P_1
P_2
$\ldots$
P_{k-1}
P_k
$\langle N_1, e_1 \rangle$
$\langle N_2, e_2 \rangle$
$\langle N_{k-1}, e_{k-1} \rangle$
$\langle N_k, e_k \rangle$

Håstad's Broadcast Attack

Suppose $e_i = 3 \quad \forall i \in \{1, 2, \ldots, k\}, \quad k \geq 3.$
Marvin obtains: C_1, C_2, C_3 where:

$$C_1 \equiv M^3 \pmod{N_1}$$

$$C_2 \equiv M^3 \pmod{N_2}$$

$$C_3 \equiv M^3 \pmod{N_3}$$

Håstad's Broadcast Attack

Suppose $e_i = 3 \quad \forall i \in \{1, 2, \ldots, k\}, \quad k \geq 3.$
Marvin obtains: C_1, C_2, C_3 where:

$$C_1 \equiv M^3 \pmod{N_1}$$

$$C_2 \equiv M^3 \pmod{N_2}$$

$$C_3 \equiv M^3 \pmod{N_3}$$

Then from CRT we have:

$$C' \equiv M^3 \pmod{N_1 N_2 N_3} \quad M^3 < N_1 N_2 N_3$$

Håstad's Broadcast Attack

Suppose $e_i = 3 \quad \forall i \in \{1, 2, \ldots, k\}, \quad k \geq 3.$
Marvin obtains: C_1, C_2, C_3 where:

$$C_1 \equiv M^3 \pmod{N_1}$$

$$C_2 \equiv M^3 \pmod{N_2}$$

$$C_3 \equiv M^3 \pmod{N_3}$$

Then from CRT we have:

$$C' \equiv M^3 \pmod{N_1 N_2 N_3} \quad M^3 < N_1 N_2 N_3$$

$$\Longrightarrow \; M = \sqrt[3]{C'}$$

Håstad's Broadcast Attack

Suppose that for each participant P_i, Bob has a fixed polynomial $f_i \in \mathbb{Z}_{N_i}[x]$.

$$M \to (f_i(M))^{e_i} = C_i$$

Suppose that Marvin learns C_i.
Håstad showed that if enough parties are involved, Marvin can recover M.

Håstad's Broadcast Attack

Theorem (Håstad)

Let $N_1, \ldots, N_k$ be pairwise relatively prime integers, and set $N_{min} = min_i(N_i)$. Let $g_i \in Z_{N_i}[x]$ be k polynomials of maximum degree δ. Suppose there exists a unique $M < N_{min}$ satisfying

$$g_i(M) \equiv 0 \pmod{N_i} \quad \text{for all } i = 1, \ldots, k.$$

Under the assumption that $k > \delta$, Marvin can efficiently find M given $\langle N_i, g_i \rangle_{i=1}^{k}$.

Håstad's Broadcast Attack

Proof.

$$\bar{N} := N_1 N_2 \cdots N_k$$

Håstad's Broadcast Attack

Proof.

$$\bar{N} := N_1 N_2 \cdots N_k$$

WLOG, g_i is monic and $\deg g_i = \delta \quad \forall i = \{1, 2. \ldots, k\}$.

Håstad's Broadcast Attack

Proof.

$$\bar{N} := N_1 N_2 \cdots N_k$$

WLOG, g_i is monic and $\deg g_i = \delta \quad \forall i = \{1, 2. \ldots, k\}$.

$$g(x) := \sum_{i=1}^{k} T_i g_i(x),$$

$$T_i = \begin{cases} 1 \bmod N_j, & i = j \\ 0 \bmod N_j, & i \neq j \end{cases}$$

Håstad's Broadcast Attack

Proof.

$$\bar{N} := N_1 N_2 \cdots N_k$$

WLOG, g_i is monic and $\deg g_i = \delta \quad \forall i = \{1, 2. \ldots, k\}$.

$$g(x) := \sum_{i=1}^{k} T_i g_i(x),$$

$$T_i = \begin{cases} 1 \bmod N_j, & i = j \\ 0 \bmod N_j, & i \neq j \end{cases}$$

g is monic $\pmod{\bar{N}}$, $\quad g(M) = 0 \pmod{\bar{N}}$

$$M < N_{min} \leq \bar{N}^{\frac{1}{k}} < N^{\frac{1}{\delta}}$$

Conclusion - Use random padding !

Coppersmith's Short Pad Attack

Suppose $e = 3$; R, R' random pads such that $R' = R + r$, where $|r| < N^{\frac{1}{9}}$; $M \in \mathbb{Z}_N^*$

$$c \equiv m^3 \equiv (2^k M + R)^3 \pmod{N}$$
$$c' \equiv (m')^3 \equiv (2^k M + R')^3 \equiv (m + r)^3 \pmod{N}$$

Coppersmith's Short Pad Attack

Suppose $e = 3$; R, R' random pads such that $R' = R + r$, where $|r| < N^{\frac{1}{9}}$; $M \in \mathbb{Z}_N^*$

$$c \equiv m^3 \equiv (2^k M + R)^3 \pmod{N}$$
$$c' \equiv (m')^3 \equiv (2^k M + R')^3 \equiv (m + r)^3 \pmod{N}$$

Eliminating m:
$Res_m(m^3 - c, (m + r)^3 - c') =$

Coppersmith's Short Pad Attack

Suppose $e = 3$; R, R' random pads such that $R' = R + r$, where $|r| < N^{\frac{1}{9}}$; $M \in \mathbb{Z}_N^*$

$$c \equiv m^3 \equiv (2^k M + R)^3 \pmod{N}$$
$$c' \equiv (m')^3 \equiv (2^k M + R')^3 \equiv (m + r)^3 \pmod{N}$$

Eliminating m:
$Res_m(m^3 - c, (m + r)^3 - c') =$
$r^9 + (3c - 3c')r^6 + (3c^2 + 21cc' + 3(c')^2)r^3 + (c - c')^3 \equiv 0 \pmod{N}$
$|r| < N^{\frac{1}{9}} \rightarrow$ recover r with Coppersmith's method
And then use Franklin-Reiter method to recover m.

Partial Key Exposure

Suppose we have obtained 300 least significant bits of d; $e = 2^{16} + 1$

Partial Key Exposure

Suppose we have obtained 300 least significant bits of d; $e = 2^{16} + 1$
We want to factorize N.

Partial Key Exposure

Suppose we have obtained 300 least significant bits of d; $e = 2^{16} + 1$
We want to factorize N.

$$ed - k\phi(N) = 1, \ \mathrm{k} < e$$
$$ed - k(N - p - q + 1) = 1$$
$$ed - k(N - p - q + 1) \equiv 1 \pmod{2^l}, \ \text{for l} \in 1, \cdots, 300$$
$$ped - k(pN - p^2 - N + 1) \equiv p \pmod{2^l}$$

Partial Key Exposure

Suppose we have obtained 300 least significant bits of d; $e = 2^{16} + 1$
We want to factorize N.

$$ed - k\phi(N) = 1, \ \mathrm{k} < e$$
$$ed - k(N - p - q + 1) = 1$$
$$ed - k(N - p - q + 1) \equiv 1 \pmod{2^l}, \ \text{for l} \in 1, \cdots, 300$$
$$ped - k(pN - p^2 - N + 1) \equiv p \pmod{2^l}$$

$\rightarrow$ obtain 300 least significant bits of p

Partial Key Exposure

Suppose we have obtained 300 least significant bits of d; $e = 2^{16} + 1$
We want to factorize N.

$$ed - k\phi(N) = 1, \ \mathrm{k} < e$$
$$ed - k(N - p - q + 1) = 1$$
$$ed - k(N - p - q + 1) \equiv 1 \pmod{2^l}, \ \text{for l} \in 1, \cdots, 300$$
$$ped - k(pN - p^2 - N + 1) \equiv p \pmod{2^l}$$

$\rightarrow$ obtain 300 least significant bits of p
$p = rx + t$, where $r = 2^{300}$, t known

Partial Key Exposure

Suppose we have obtained 300 least significant bits of d; $e = 2^{16} + 1$
We want to factorize N.

$$ed - k\phi(N) = 1, \ \mathrm{k} < e$$
$$ed - k(N - p - q + 1) = 1$$
$$ed - k(N - p - q + 1) \equiv 1 \pmod{2^l}, \text{ for l } \in 1, \cdots, 300$$
$$ped - k(pN - p^2 - N + 1) \equiv p \pmod{2^l}$$

$\rightarrow$ obtain 300 least significant bits of p
$p = rx + t$, where $r = 2^{300}$, t known

$$\text{We compute } r^{-1} \pmod{N}$$
$$r^{-1}p = x + r^{-1}t \equiv 0 \pmod{p}$$
$$f(x) := x + r^{-1}t \equiv 0 \pmod{N}$$

Thank you for your attention!