

Летняя школа - конференция

"Криптография и информационная
безопасность", 2023

г. Калининград

Практический криптобанк RSA

Сергей Гребнев

sg@qapp.tech

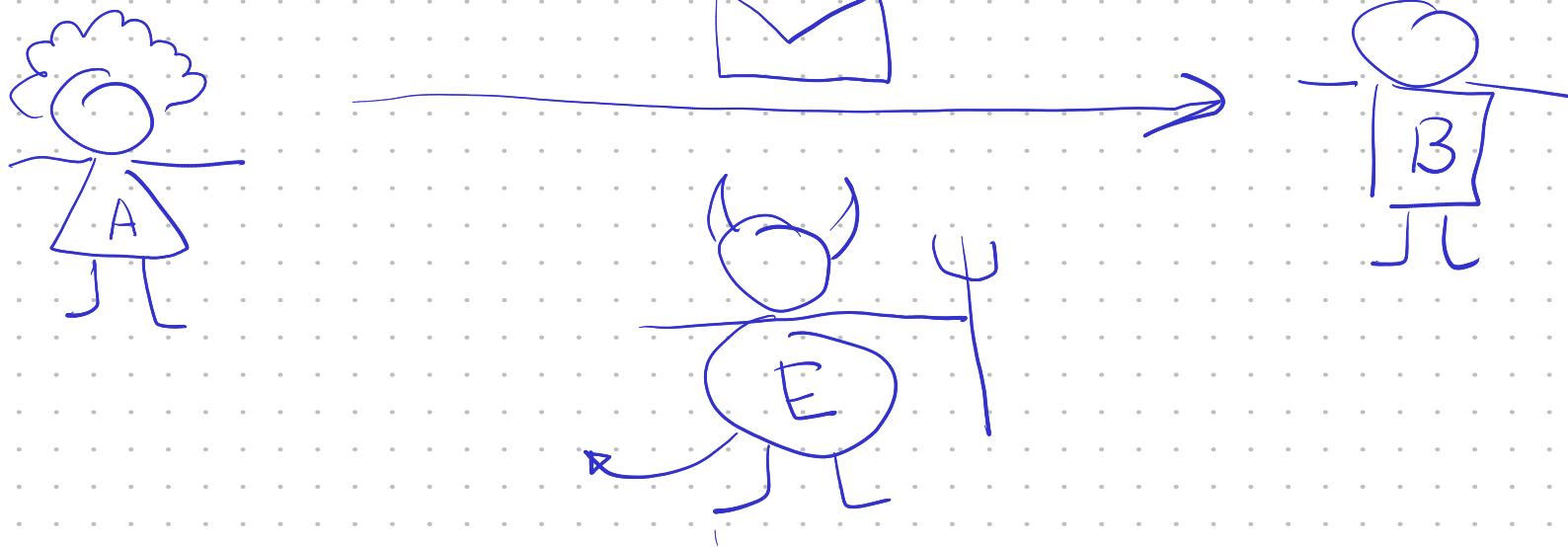


QApp

KyAnn, Москва

I. RSA

- принципы и методы криптографии с открытым ключом
- Теория чисел и RSA
- Криптоанализ



- конфиденциальность
- целостность
- подтверждение авторства

Классика: симметричные схемы



$$D_k(E_k(M)) = M$$

Шифр Венгра: $C = M \oplus K$

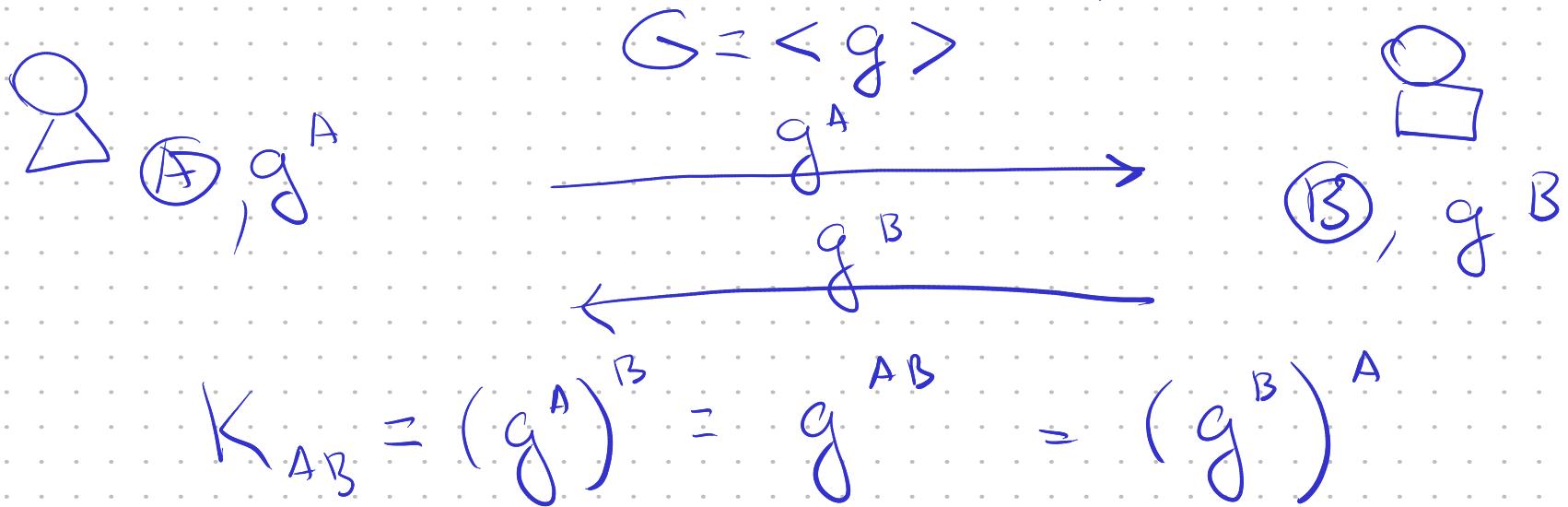
Чинов, Котельников:

- 1) $|M| = |K|$
- 2) $K \in_R V^*$

абсолютное теоретико-информационное
состество!

А если канал открыт?

- 1976, Диффи-Хеллман-Меркель:



- DHP: Дано g^A, g^B - найти g^{AB}

- DLP: Дано g^x , найти x

Пример $G = GF(p)$; $G = E(GF(p))$

(*) Нечасев, Генгфонг: 1960-е

1978

Rivest
Shamir
Adleman

} RSA *

Konbujo Barzob mod N:

$$a, b \in \mathbb{Z}$$

$$a+b : (a+\beta) \circ_b N$$

$$a * b : (a * \beta) \circ_b N$$

$$a^* : (\underbrace{a * a * \dots * a}_\text{* pag}) \circ_b N$$

$$\left| \begin{array}{l} a \equiv \beta \pmod{N} \\ \text{even} \\ (a - b) \% N = 0 \end{array} \right.$$

(*) Koc, 1973

$\varphi(N)$: Функция Эuler'a:

1) Многоточечный набор: если $\text{GCD}(x, y) = 1$, то
 $\varphi(xy) = \varphi(x)\varphi(y)$

2) $p \in \mathbb{P} \Rightarrow \varphi(p) = p - 1$

3) $\varphi(p^k) = (p-1)p^{k-1}$

$\varphi(N) = |\{x \in \{1, \dots, N-1\} : \text{GCD}(x, N) = 1\}|$

Теорема : $\forall a \in \{1, \dots, N-1\},$
 $a^{\varphi(N)} \equiv 1 \pmod{N}$

$N = p \cdot q \Rightarrow \varphi(N) = (p-1)(q-1)$

(schoolbook)

RSA:

1. Выработка ключа:

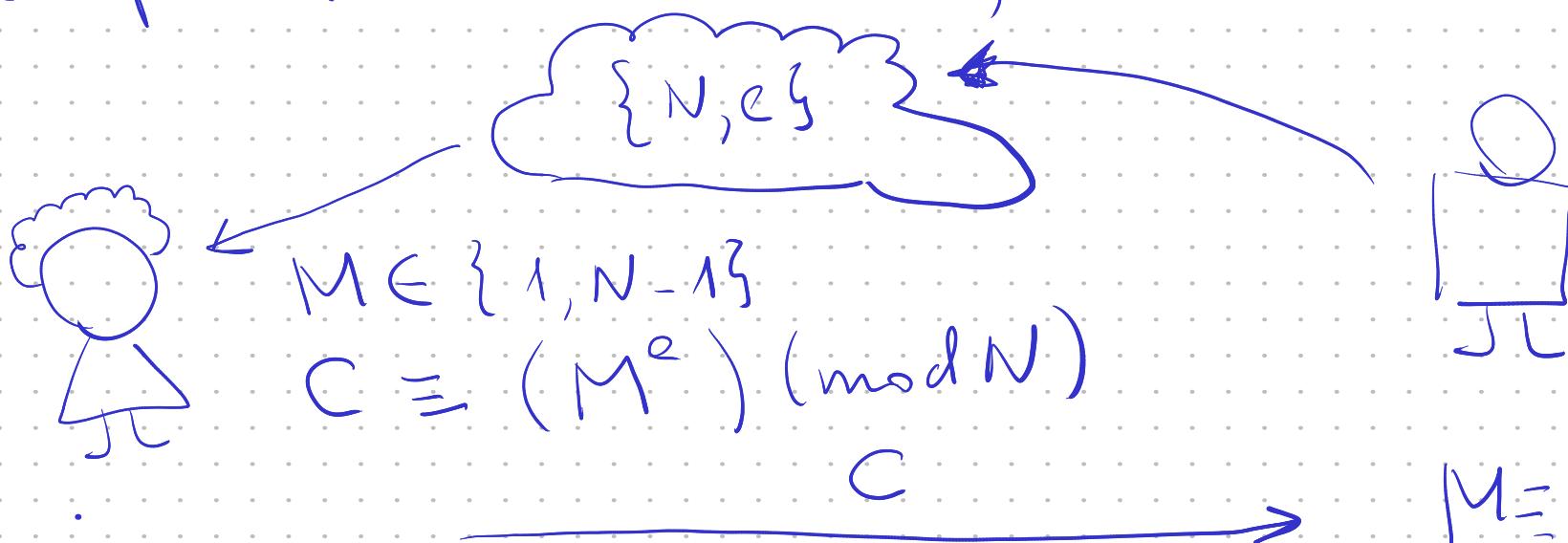
$$p, q \in \mathbb{P} ; p \neq q ; N = p \cdot q ;$$

$$e, d : ed \equiv 1 \pmod{\varphi(N)}$$

Секретный ключ: p, q, d

Открытый ключ: N, e

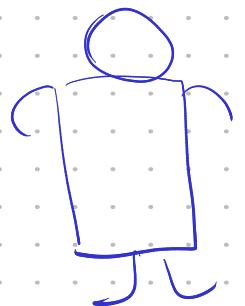
2.



$$\begin{aligned} M &= C^d \equiv \\ &\equiv (M^e)^d \stackrel{ed}{=} M \equiv M \pmod{N} \end{aligned}$$

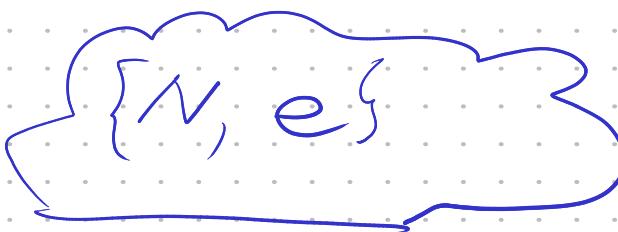
Рогнунс RSA:

"однажды" испортил



$$N = p \cdot q;$$

$$e, d: ed \equiv 1 \pmod{\varphi(N)}$$



$$M \in \{1, \dots, N-1\}$$

$$\gamma(M) = M^d \pmod{N}$$

$$M \xrightarrow{\gamma(M)}$$

$$\dots \xleftarrow{g^a}$$

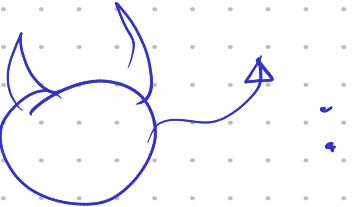
$$M \stackrel{?}{=} (\gamma(M))^c \pmod{N}$$

(рогнунс с бессознательной ошибкой)

нет

Пример:

Этап	Описание операции	Результат операции
Генерация ключей	Выбрать два простых различных числа	$p = 3557,$ $q = 2579$
	Вычислить произведение	$n = p \cdot q = 3557 \cdot 2579 = 9173503$
	Вычислить функцию Эйлера	$\varphi(n) = (p - 1)(q - 1) = 9167368$
	Выбрать открытую экспоненту	$e = 3$
	Вычислить секретную экспоненту	$d = (k \cdot \varphi(n) + 1)/e$ $= (2 \cdot 9167368 + 1)/3$ $= 6111579$
	Опубликовать открытый ключ	$\{e, n\} = \{3, 9173503\}$
Шифрование	Сохранить закрытый ключ	$\{d, n\} = \{6111579, 9173503\}$
	Выбрать текст для зашифрования	$m = 111111$
Расшифрование	Вычислить шифротекст	$c = E(m)$ $= m^e \pmod{n}$ $= 111111^3 \pmod{9173503}$ $= 4051753$
	Вычислить исходное сообщение	$m = D(c) =$ $= c^d \pmod{n}$ $= 4051753^{6111579} \pmod{9173503}$ $= 111111$

(с) Викинеги
 : $N, e \rightsquigarrow p, q = ?$ (FACT)
 $d = ?$ (загадка RSA)

Прегнотение

FACT - "сноска"

(например, FACT ∈ NP)

Сложность: $O(f(n))$ операций

На 1978 год: алгоритм F оценка

$O(\sqrt{N}(\ln \ln N)^2)$ (нейлон) "million years to break"

1990-е: NFS:

$$L_N[\alpha; c] = \exp\left(c + \bar{O}(1)\right) \left((\ln N)^{\frac{\alpha}{2}} (\ln \ln N)^{\frac{1-\alpha}{2}}\right)$$

(суперэкспоненциальная оценка) | $c \approx 1.923$
 $\alpha = 1/3$

1994, Шор: $O(\log^3 N)$ операций, $O(\log N)$ кубиков
(аналогичная оценка в квантовом режиме)

2023, L'huillier et al.: суперлинейная оценка - рекорд!

RSA \sim FACT : neglects

Theorem 9 Есмъ N , $\varphi(N)$ то ѝ епрекъмвър
беспръсточник акощо a е изпомъ φ -когоригащо N

$a \in_R \{1, N-1\}$; $N > \text{GCD}(a^{\varphi(N)-1}, N) > 1$? $\xrightarrow{\text{да}}$ наима генове

нет

Есмъ d, e , то $\exists k$ $k \cdot \varphi(N) = ed - 1$

Утак. "однажды" атака на RSA:

$$\text{FACT}(n) \xrightarrow{\quad} \{p, q\} \xrightarrow{\quad} d$$

CS'95 Metagrob

факторизацией

- Басуренко О. Н. "Теоретико-числовые алгоритмы в криптографии", 2005
- Сонг Ян "Криптоанализ RSA": 2008
- Martin J. Klimek "Cryptanalysis of RSA and its Variants": 2009
- Song Yan "Quantum Computational Number Theory": 2015

Ле^ре^дор (предыдущие генетики)

Меня Ферма

P±1 ; ECM (Ленсфар)

Dukcon

Квадратичное уравнение

! Решение уравнений многочленов

Уравнение групп

MPQS

! Меня Шор

Мережа Репна

$$[N = p \cdot q, p \approx q]$$

Угода: якщо $x = \frac{1}{2}(p+q)$, $y = \frac{1}{2}(p-q)$

тоді $N = x^2 - y^2 = (x-y)(x+y)$
також $y^2 = N - x^2$

1) $k = \lfloor \sqrt{N} \rfloor + 1$, $y = k^2 - N$

2) ~~Если~~ $\lfloor \sqrt{y} \rfloor = \sqrt{y}$: непарні k (y), where $y = y + 2k + d$,
 $d = d + 2$

3) ~~если~~ $\lfloor \sqrt{y} \rfloor < N/2$: непарні k (z), where: непарні k (5)

4) $x = \sqrt{N+y}$, $y = \sqrt{y}$; print $(x-y, x+y)$

5) EXIT // FAIL

Відомо: $|p-q|$ єдною з двох "не співком
мандаток"

Pt 1 - metoda

Найти N -квадратиче

- 1) $a \in \mathbb{Z}_N^*$; $k = \text{LCM}(1, 2, \dots, B)$
- 2) $a_k \equiv a^k \pmod{N}$
- 3) $\exists m \quad 1 < \text{GCD}(a_k - 1, N) \quad - \underline{\text{член}}$
- 4) Умножить, непрерывно k many (1)

Сложность: $O(B \log B (\log N)^2)$

Метод Ленгаура (ECM)

Эллиптические кривые $(*)$ $y^2 \equiv x^3 + ax + b \pmod{p}$

Группа (aSemb) ; $E(\mathbb{Z}_N)$ - мн-ло нср (x, y) ;
условие целочисленных $(*)$

1) Справимся с кратностью 2, т.к. $E(\mathbb{Z}_N), P(x, y) \in E$

2) $k = \text{LCM}(2, \dots, 3)$

3) "burnside" к P

- B проекции на δ . сингулярн, когдк нумер
"делим" - атт. Ebungen geht непримарно
нормир

Оценка: $L_p \left[\frac{1}{2}, \sqrt{2} \right]$

Метод решения

Цель: искать X, Y две факториальные решения не неравенством!

I. Выбор параметров: B -максимум факторных выражений

$$B = \{-1, P_1, \dots, P_k \leq B\}$$

II. Проектирование: a_1, \dots, a_k — B -заявки

$$\begin{cases} a_1 = (-1)^{k_{-1,1}} P_1^{k_{1,1}} \cdots P_\ell^{k_{\ell,1}} \\ \cdots \\ a_k = (-1)^{k_{-1,k}} P_1^{k_{1,k}} \cdots P_\ell^{k_{\ell,k}} \end{cases} \rightarrow X = \prod_{i \in U} a_i; \quad Y = \prod_{i \in U} P_i^{k_{i,j}}$$

III. Аналитика ансамбля:

$$\begin{pmatrix} k_{-1,1} & k_{1,1} & \cdots & k_{\ell,1} \\ \vdots & & & \\ k_{-1,\ell} & k_{1,\ell} & \cdots & k_{\ell,\ell} \end{pmatrix} \cdot U \equiv 0 \pmod{2},$$

IV. Содействие X, Y , биномиальный $\text{GCD}(X \pm Y, N)$

GNFS:

I. $f_1, f_2 : f_1(m) \equiv f_2(m) \equiv 0 \pmod{N}$
 $f(\alpha_1) = 0, f(\alpha_2) = 0 \quad \alpha_i \in \mathbb{F}$

$$\begin{array}{ccc} \varphi_1 : \mathbb{Z}[\alpha_1] & \longrightarrow & \mathbb{Z}_N \\ & \alpha_1 \mapsto & m \\ & \downarrow & \swarrow \\ & m & \end{array} \quad \begin{array}{ccc} \varphi_2 : \mathbb{Z}[\alpha_2] & \longleftarrow & \\ & \alpha_2 \mapsto & \end{array}$$

II. Проверка: (c, d) т.е. $N(c-d\alpha_1), N(c-d\alpha_2)$ неприводимы
 в \mathbb{Z} -множестве

III. Несколько примеров: $S_{1,2} = \bigcap_{i \in S} (c_i - d_i \alpha_1) = \bigcap_{i \in S} (c_i - d_i \alpha_2) =$
 Шагратко проверяется неприводимость

IV. Итак, если $x \in S_{1,2}$, то $x \in \text{ker } \varphi_1 \cap \text{ker } \varphi_2$
 $\text{ker } \varphi_1 = \langle c - d\alpha_1 \rangle$ и $\text{ker } \varphi_2 = \langle c - d\alpha_2 \rangle$

Рекорды факторизации

Год	Число	Битов	Метод	Время
1991	RSA-100	330	MPQS	Approx. 7 MIP-Years
1992	RSA-110	364	MPQS	N/A
1993	RSA-120	397	MPQS	Approx 835 MIPS-Years
1994	RSA-129	426	MPQS	Approx. 5000 MIPS-Years
1996	RSA-130	430	GNFS	Approx. 500 MIPS-Years
1999	RSA-140	463	GNFS	Approx. 2000 MIPS-Years
2004	RSA-150	496	GNFS	N/A
1999	RSA-155	512	GNFS	8000 MIPS-Years
2003	RSA-160	530	GNFS	N/A
2009	RSA-170	563	GNFS	N/A
2003	RSA-174	576	GNFS	N/A
2010	RSA-180	596	GNFS	N/A
2010	RSA-190	629	GGNFS	N/A
2005	RSA-193	640	GNFS	30 CPU core-years
2005	RSA-200	663	GNFS	55 CPU core-years
2013	RSA-210	696	GGNFS	N/A
2012	RSA-212	704	NFS	500 CPU core-years
2016	RSA-220	729	NFS	N/A
2018	RSA-230	762	NFS	N/A
2020	RSA-232	768	NFS	50 CPU core-years
2009	RSA-232	768	NFS	2000 CPU core-years
2019	RSA-240	795	NFS	900 CPU core-years
2020	RSA-250	829	GNFS	2700 CPU core-years

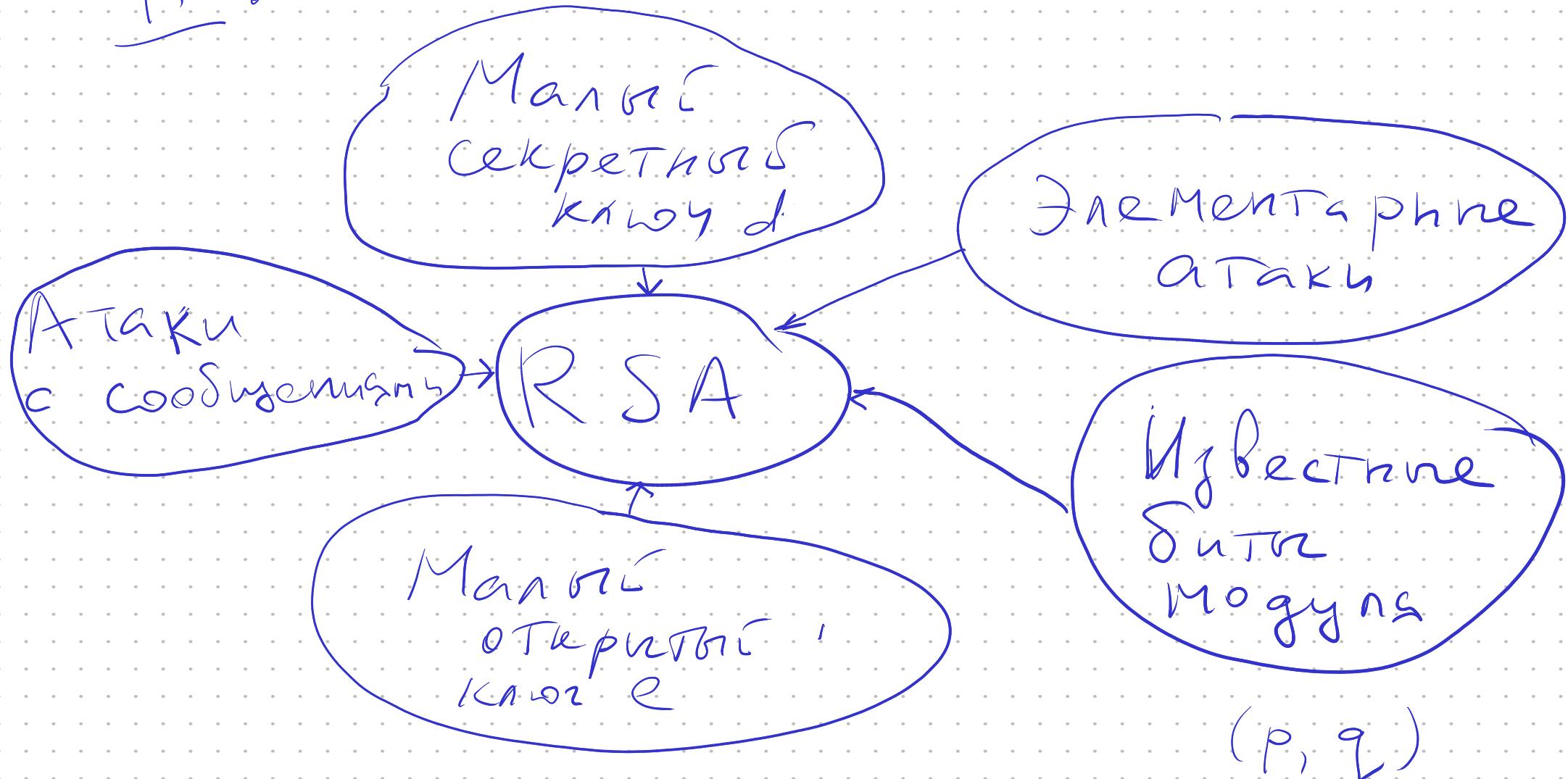
Год	Число	Разрядность	Метод
2001	15	4	Шор (3)
2012	21	5	Шор (5)
2014	3599	16	Шор (Сим)
2014	11663	16	Шор (Сим)
2014	56153	16	Шор (Сим)
2014	175	8	Шор (5)
2023	1961	11	Шнор (3)
2023 (*)	48567227	26	Шнор (5)
2023	261980999226229	48	Шнор (10)

Рекордн. факторијачи

(*) - не подтверждено: QApp + QBoard,
Google

II.

ПакТука



Спирал маюро e.

$$e = 3, 17, 2^{16} + 1$$

Доказате багаємо в іншому!

Пусть $M \ll N^{\frac{1}{3}}$; тоді $C < N$, $M = (c)^{\frac{1}{3}}$

Гомоморфізм

$$E(m_1 m_2) = E(m_1) E(m_2)$$

Однини множин $\{N, e_1\} \xrightarrow{\varphi(N)} \varphi(N)$

$$\{N, e_2\} \dashrightarrow \overbrace{(d_2)}^{\downarrow}$$

Однини складних кіль

$$N_1 = p_1 q, \quad N_2 = p_2 q$$

$$\text{GCD}(N_1, N_2) = \boxed{q}$$

Эквивалентные классы:

$\lambda(N)$ - фундаментальная функция Картина: если $N = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_n^{\alpha_n}$,
 тогда $\lambda(N) = \text{LCM}(\lambda(2^{\alpha_0}), \lambda(p_1^{\alpha_1}), \dots, \lambda(p_n^{\alpha_n}))$;

$\lambda(2) = 1$; $\lambda(p) = p-1$;

$\lambda(2^\alpha) = \frac{1}{2}(2^\alpha - 1)$; $\lambda(p^\alpha) = (p-1)p^{\alpha-1}$

Тогда для пары (e, d) know bugs
 $(e, d + k\lambda(N))$ - эквивалентны.

Алгоритм Хаккага: $(N_1, e) : m^e \xleftarrow[m \pmod{N_1}]{} \quad$

$(N_k, e) : m^e \xleftarrow[m \pmod{N_k}]{} \quad$

↓ K.T.O.

$m^e \pmod{N_1 \cdots N_k}$

Если $N_1 \cdots N_k \gg N_1^e$ — можно $m = c^{1/e}$

Случай малого d

Теорема (Bunep, 1990): Рассмотрим $d < \frac{1}{c}N^{\frac{1}{4}}$, $c > 1$;
 Тогда можно определить d из $\{N, e\}$ за
 полиномиальное время

$$c \approx 3$$

Иdea: использовать генераторы групп

$$a \in \mathbb{R}; a = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}} \in [a_0; a_1, a_2, \dots]$$

Некоторые некомпактные группы $[a_0; \dots, a_n]$ в
 $\frac{e}{N}$ имеет форму $\frac{k}{d}$. При сокращении
 получим Теорему, включающую малое.

Оптимизация: решетка и LLL-алгоритм

Teorems (Бонн-Дюрфи). Для модуса $\varepsilon > 0$

существует но Таке, такое $N = pq$, $p \approx q$,
так что $N = n$, то $e = N^\alpha$, $d = N^\delta$ и

$\delta < \frac{7}{6} - \frac{1}{3}\sqrt{1-6\varepsilon} - \varepsilon$, то N факторизуется в
множестве чисел

Cryptohme. RSA - шифровка при $\delta < 0.2847 - \varepsilon$

Решётка гиперплоскость (Боннер-Манн):

$$\delta < 0.2899 - \varepsilon$$

Teorema Konneccanta

Teorema Pyros $b \mid N; b > N^{\beta}$. Pyros $f_b(x)$ -
monozornen crenem: $d, c > 1$ -konstanta. Toys b e
 x_0 tame, zo $f_b(x_0) \equiv 0 \pmod{N}$ u $|x_0| \leq N^{B^2/d}$
M.S. našejem γ monozornen or $d, c = \log N$
lopmi.

Cygolne $b \mid N, \tilde{b} = k b + x_0$.

$$f(x) = \tilde{b} + x$$

$$f_r(x) = (\tilde{b} + x)^r$$



$$f_r(x_0) \equiv 0 \pmod{N} \rightarrow x_0;$$

$$\text{GCD}(N, \tilde{b} - x_0) > 1$$

Спору пажне аппроксимацији p -факторијам $N!$

Spannrechnung Kerzen

Heninger et al., 2012

	SSL Observatory (12/2010)	Our TLS scan (10/2011)	Our SSH scans (2-4/2012)
Hosts with open port 443 or 22	≈16,200,000	28,923,800	23,237,081
Completed protocol handshakes	7,704,837	12,828,613	10,216,363
Distinct RSA public keys	3,933,366	5,656,519	3,821,639
Distinct DSA public keys	1,906	6,241	2,789,662
Distinct TLS certificates	4,021,766	5,847,957	—
Trusted by major browsers	1,455,391	1,956,267	—

	Our TLS Scan	Our SSH Scans
Number of live hosts	12,828,613 (100.00%)	10,216,363 (100.00%)
... using repeated keys	7,770,232 (60.50%)	6,642,222 (65.00%)
... using vulnerable repeated keys	714,243 (5.57%)	981,166 (9.60%)
... using default certificates or default keys	670,391 (5.23%)	
... using low-entropy repeated keys	43,852 (0.34%)	
... using RSA keys we could factor	64,081 (0.50%)	2,459 (0.03%)
... using DSA keys we could compromise		105,728 (1.03%)
... using Debian weak keys	4,147 (0.03%)	53,141 (0.52%)
... using 512-bit RSA keys	123,038 (0.96%)	8,459 (0.08%)
... identified as a vulnerable device model	985,031 (7.68%)	1,070,522 (10.48%)
... model using low-entropy repeated keys	314,640 (2.45%)	

Lensstra et al., 2012

Table 1. Most frequently occurring RSA public exponents.

X.509		PGP		Combined	
e	%	e	%	e	%
65537	98.4921	65537	48.8501	65537	95.4933
17	0.7633	17	39.5027	17	3.1035
3	0.3772	41	7.5727	41	0.4574
35	0.1410	19	2.4774	3	0.3578
5	0.1176	257	0.3872	19	0.1506
7	0.0631	23	0.2212	35	0.1339
11	0.0220	11	0.1755	5	0.1111
47	0.0101	3	0.0565	7	0.0596
13	0.0042	21	0.0512	11	0.0313
65535	0.0011	$2^{127} + 3$	0.0248	257	0.0241
other	0.0083	other	0.6807	other	0.0774

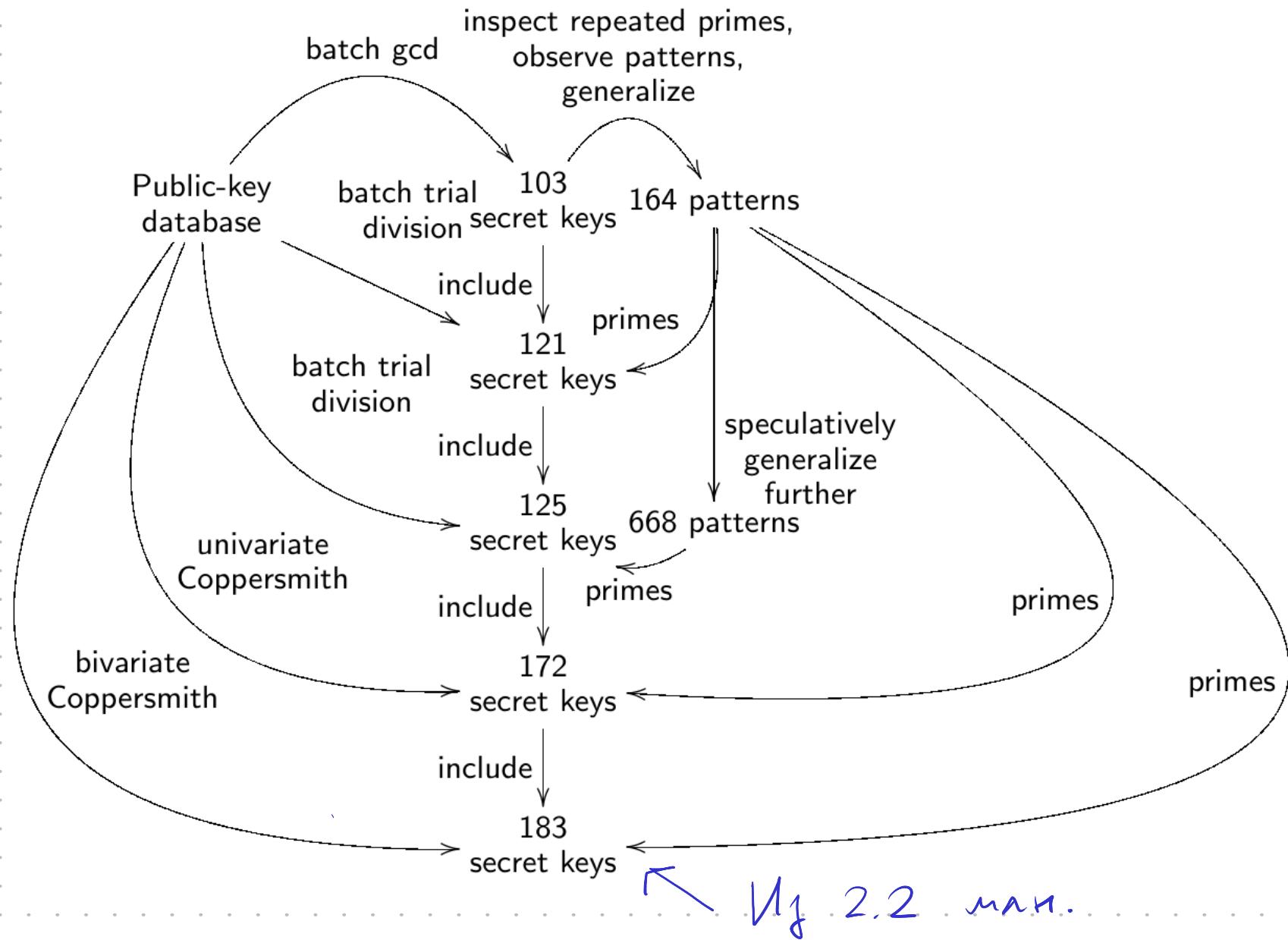
Bernstein, 2013: kein с тангенциальными
экспонентами настройками

a) 103 ключа из 2.26 млн

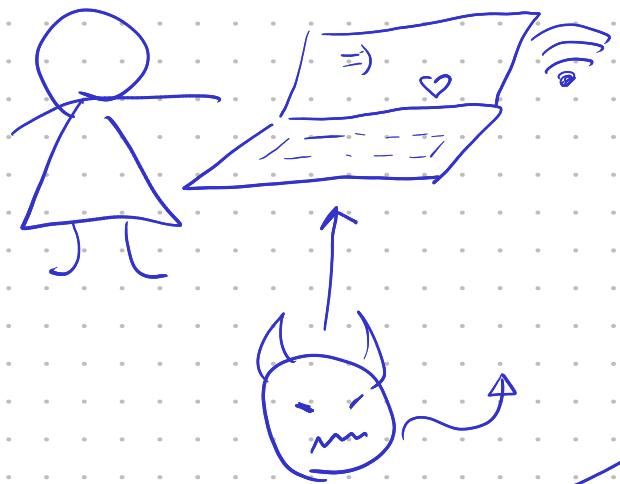
б) модуль б ГПСЧ → есть 18 новых Р

в) Метод Коннектита — есть 39 новых Р

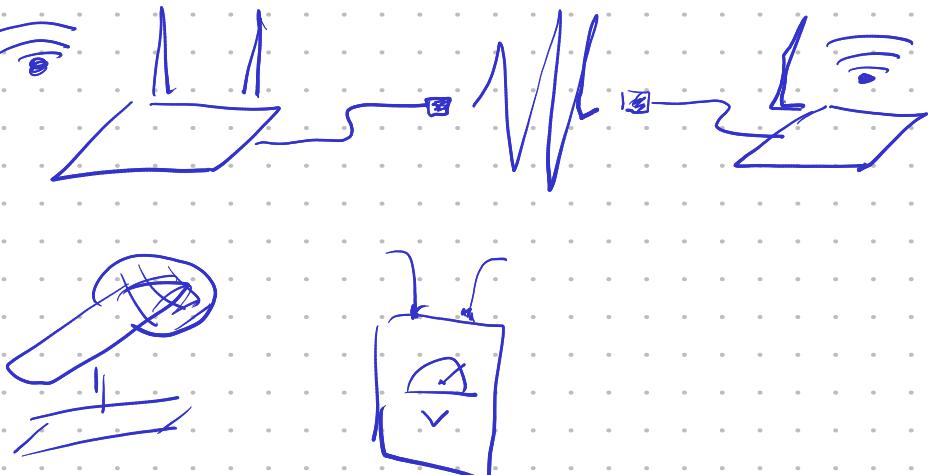
Q. Suri's εδγρ peyntata



Атаки по побочному каналу



ассивные:



активные

Часы информации
о кэше

алгоритм

Конфиденциальность

Дай:
Некорректные неживые -
информации о кэше

Шамиль и др.: определение кэша OpenSSL
оборудование: микрофон за \$20!

Бытлоги

- 1) Плохая ли RSA сама по себе?
- 2) Где основные ошибки? - ГНСЧ
- 3) Альтернативы:
 - ECC
 - PQC
- 4) Квантовые компьютеры:

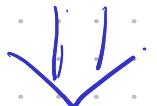


(2028 + 2.2.)

(RSA-2048: 20 ман кубиков, 8 раков)

Э: ~1000 кубиков (IBM Osprey)

Метод Шора - работает!



Постквантовый мир подходит!

Cracuso je Brunanue!

?

?

?

(c) 2023 Cepres Frednel, sg@qapp.tech