Crypto for ~~Crypto~~ Computational Number Theory:
Certifying Giant Nonprimes

Charlotte Hoffmann[1], Pavel Hubáček[2], Chethan Kamath[3], Krzysztof Pietrzak[1]

[1]Institute of Science and Technology Austria
[2]Charles University, Faculty of Mathematics and Physics
[3]Tel Aviv University

Giant Prime Numbers

- GIMPS and PrimeGrid: large-scale projects dedicated to searching giant prime numbers
- Expensive p . Proth, Mersenne)
- Prevent che
  - Double ch
  - Cryptogra

30027491 PrimeGrid

ject cover running costs for this month

PrimeGrid Mega Primes

Page 1 of 2 > Last page

	Prime	Digits	Discoverer	Team	Date
1	10223*2^31172165+1	9,383,761 (decimal)	SyP (primes)		2016-10-31 22:13:54 UTC
2	1963736^1048576+1	6,598,776 (decimal)	tng (primes)	Antarctic Crunchers	2022-09-24 15:01:43 UTC
3	1951734^1048576+1	6,595,985 (decimal)	apophise@jisaku (primes)	Team 2ch	2022-08-09 11:56:02 UTC
4	202705*2^21320516+1	6,418,121 (decimal)	Pavel Atnashev (primes)	Ural Federal University	2021-11-25 03:19:26 UTC

Proth Numbers

$$\boldsymbol{N = k2^n + 1}$$

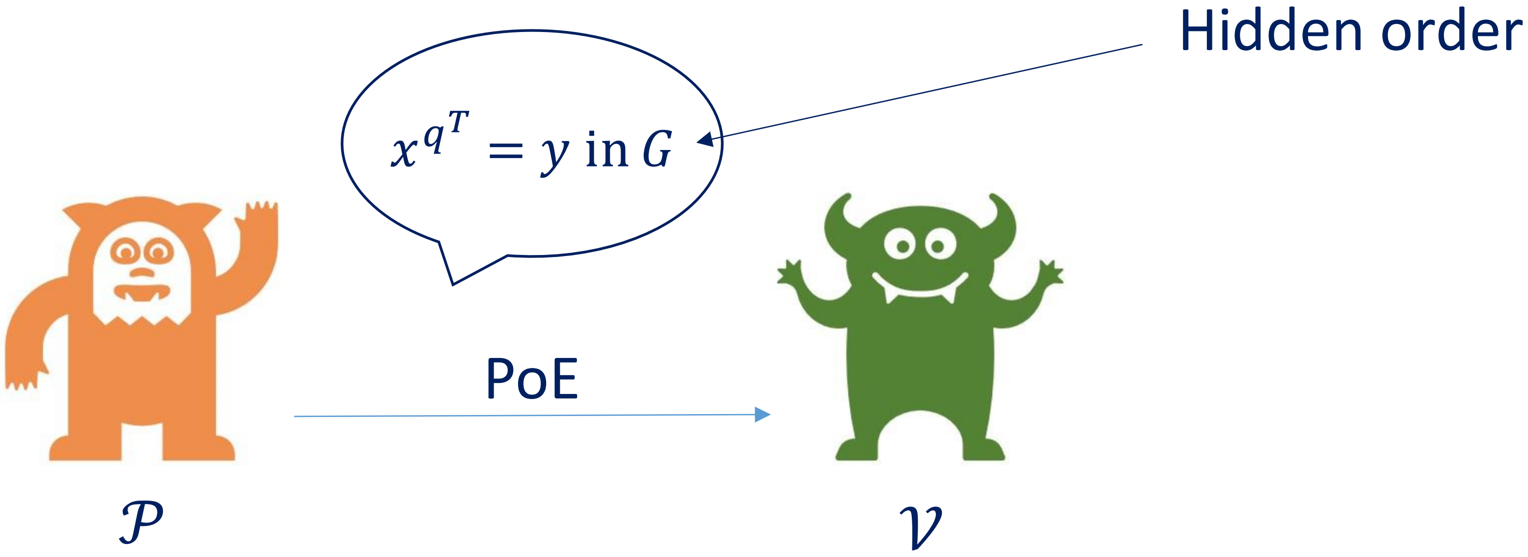
$$n \in \mathbb{N}, k < 2^n \text{ odd}$$

<u>Proth's Theorem</u>

For all x quadratic non-residue mod N:

$$N \text{ prime} \Leftrightarrow x^{k2^{n-1}} = -1 \bmod N$$

Proofs of Exponentiation



- If $\mathrm{ord}(G)$ is known: $\mathcal{P}$ and $\mathcal{V}$ compute $e := q^T \bmod \mathrm{ord}(G)$ and x^e
- $\mathcal{P}$ performs T sequential exponentiations

$$x \to x^q \to x^{q^2} \to x^{q^3} \to \cdots \to x^{q^T}$$

- Cost of computing and verifying the proof $\ll T$

PoEs for (Non-)Primality Certificates?

Proth's Thm: $N = k2^n + 1$

N prime $\Leftrightarrow x^{k2^{n-1}} = -1 \bmod N$

- GIMPS and PrimeGrid deployed Pietrzak's PoE to certify primality test
- BUT: Pietrzak's PoE constructed for hidden order groups
- Here: order of $\mathbb{Z}_N^*$ known for N prime

→ Attack!

Our contribution

Statistically sound certificate of **non-primality** for **Proth numbers** that

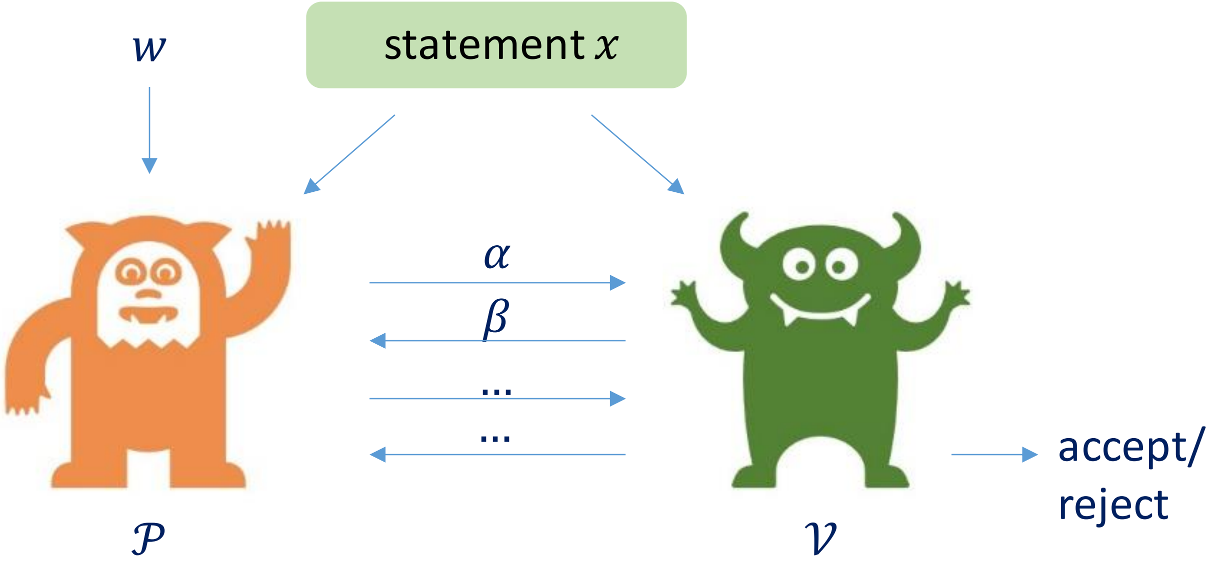
- reduces the complexity of double checking from n to $O(\lambda \log n)$
- increases the complexity of the currently deployed (not cryptographically sound) protocol by multiplicative factor 2

Technical Overview

Plan

1. Pietrzak's PoE
2. An attack in Proth number groups
3. Our protocol

Interactive Protocols



- **Soundness:** If statement is false, $\mathcal{V}$ rejects w.h.p. for every malicious $\mathcal{P}$
- **Completeness:** If statement is correct and $\mathcal{P}$ is honest, $\mathcal{V}$ accepts w.h.p.

Pietrzak's PoE [Pie19]

$$x^{2^T} = y$$

$$g_1 = x^{2^{T/2}}$$

$$\left(x^{2^{T/2}} = g_1 \right)^r \times \left(g_1^{2^{T/2}} = y \right)$$

$$r \leftarrow \$$$

$$(x^r g_1)^{2^{T/2}} = y g_1^r$$

$$g_2$$

...

$\tilde{x}^2 = \tilde{y}$? $\rightarrow$ accept/reject

Can be made non-interactive using Fiat-Shamir.

The Attack [BBF18]

Let $N = k2^n + 1$ prime
$\Leftrightarrow x^{k2^{n-1}} = -1 \bmod N$

Element of order d

$x^{k2^{n-1}} = -\alpha$

α

$r \leftarrow \$$

$(\alpha)^r \times$

g_2

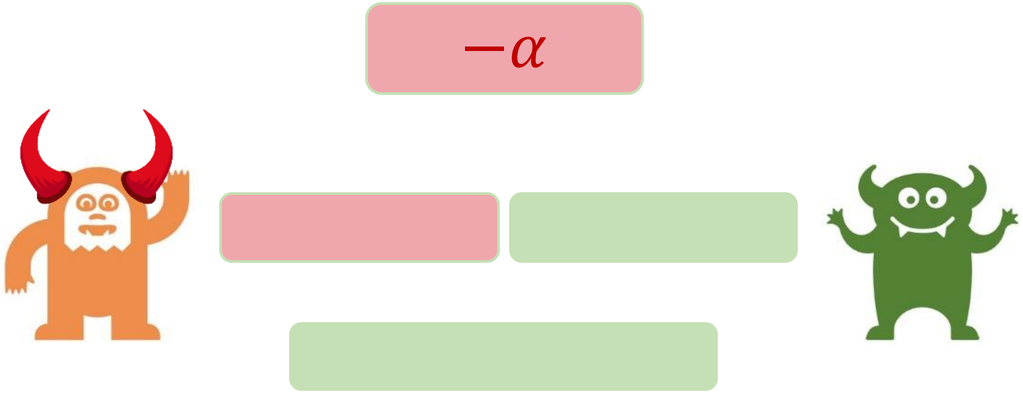
...

Holds if $\alpha^{\tilde{r}} = 1 \bmod N$

→ $\Pr[\mathcal{V}$ accepts that N is composite$] \geq 1/d$

Our Work: Observations

$$\boxed{\begin{array}{l} N = k2^n + 1 \text{ prime} \\ \Leftrightarrow x^{k2^{n-1}} = -1 \bmod N \end{array}}$$



<u>Observations:</u>

- $\mathcal{V}$ only needs to exclude that the correct result is -1
- Success probability of attack depends on order of α
- The order of α divides $N - 1 = k2^n$ if N prime

→ $\mathcal{V}$ can check if the order of α is "too small"

Our Work: Non-primality Certificate

$N = k2^n + 1$ prime
$\Leftrightarrow x^{k2^{n-1}} = -1 \bmod N$

$\neq 1$

$x^{k2^{n-1}} = -\mu$

Statistical security parameter

Case 1: $\mu^k = 1$

Case 2: $\mu^{k2^{\lambda \log n}} \neq 1$

Compute $a := 2^{-n} \bmod k$
and check if $x^k = \mu^{2a}$

accept/reject

Case 3: $\mu^{k2^{\lambda \log n}} = 1$

Pietrzak's PoE

accept/reject

[**H**HK+22]

y, Pietrzak's PoE for claim $x^{k2^{n-1-\lambda \log n}} = y$

Check if $y^{2^{\lambda \log n}} = -\mu$

accept/reject

Summary and Open Problems

weeks

Approach	Sound?	Prover's Complexity	Prover's Space	Verifier's Complexity	Proof Size
Double checking	yes	0	0	n	0
Pietrzak's PoE in $\mathbb{Z}_N^*$	no	$2\sqrt{n}$	$\sqrt{n}$	$3\lambda \log n$	$\log n$
Our work	**yes**	$\mathbf{2 \log k + \lambda \log n + 2\sqrt{n}}$	$\sqrt{\boldsymbol{n}}$	$\mathbf{\log k + 5\lambda \log n}$	$\mathbf{\log n + 1}$

hours

- We construct non-primality certificate for Proth number $k2^n + 1$
- Open: Construct cryptographically sound certificate of **primality**
- Open: Certificates of (non-)primality for other types of numbers such as Mersenne numbers $2^n - 1$

Questions?