Formally Verified Verifiable Generator

Mina A. Cyrus (Swansea University)
Mukesh Tiwari (Swansea University)

Can you vote for political elections online?

Verified 09 July 2024 - Directorate for Legal and Administrative Information (Prime Minister)

The rules are different depending on whether you vote in France, or from the foreigner:

In France | From the foreigner

You can vote via the internet provided you meet the following 3 conditions:

- You live abroad
- You are registered on a consular voters list. You can check your voter registration using this online service.
- When you registered, you provided an email address (e-mail address) and a phone number. This data is necessary to communicate a username and password.

E-Voting

In Switzerland, e-voting means voting online via the internet. E-voting is part of the Swiss e-government strategy, which entails close collaboration between the Confederation and the cantons. Since 2004, 15 cantons have offered internet voting to a limited part of their electorate in over 300 trials. The Confederation and cantons have followed the principle of 'security before speed'. In Switzerland, e-voting is only permitted if strict requirements under federal law are met.

Estonia leads world in making digital voting a reality

Baltic nation has expanded its digital revolution to include free, fair and secure online ballots

Moscow's blockchain voting system cracked a month before election

French researcher nets $15,000 prize for finding bugs in Moscow's Ethereum-based voting system.

Congress manifesto for 2024 LS polls should promise to junk EVMs, restore paper ballots: Prithviraj Chavan

Chavan, a former Maharashtra chief minister, raised the issue during deliberations in the party's panel on political issues at the three-day 'Chintan Shivir'. He said many other leaders have supported the view.

15 May, 2022, 04:10 PM IST

CNN politics The Biden Presidency Facts First 2022 Mi

Federal review says Dominion software flaws haven't been exploited in elections


By Sean Lyngaas, Evan Perez and Whitney Wild, CNN

Updated 12:18 PM EDT, Fri June 3, 2022

MOTHERBOARD
TECH BY VICE

Experts Find Serious Problems With Switzerland's Online Voting System Before Public Penetration Test Even Begins

Flaws found in NSW iVote system yet again

Analysis of source code published at the request of the NSW Electoral Commission shows that the state's election system software was still vulnerable to attack.

Blind advocates allege NSW's removal of online voting system is a breach of human rights

State electoral commission accused of discrimination for suspending iVoting platform as Blind Citizens Australia takes case to watchdog

How India conducted the world's largest election

Poll workers reach India's most remote corners to set up polling

AEC Australian Electoral Commission

1. Computer recognition (OCR/ICR/OMR) reads the preferences and other marks from the image of a scanned ballot paper.

   1a) A data entry operator populates any preferences that were unable to be read with high confidence by the computer recognition in step 1. The data entry operator also manually checks the marks read by computer recognition (for example a voter potentially identifying themselves on a ballot paper) for AEC determination.

Bootstrapping an Election

Prime p, q such that $p = 2 \times q + 1$

$$G_p = \{g^1, g^2, \ldots g^{(q-1)}\}$$

How to compute g?

$$u \leftarrow \{1 \ldots p\}$$
$$g = u^2 \mod p$$

Proof (Fermat's Little Theorem)

$$
\begin{aligned}
g^q \mod p &= (u^2)^q \mod p \\
&= u^{2\times q} \mod p \\
&= u^{p-1} \mod p \\
&= 1
\end{aligned}
$$

If we need another generator h, we can repeat the same process or

$$h = g^k \mod p \text{ for some arbitrary } k$$

Problem

Both methods are bad but the second one is disastrous if used in a commitment scheme that demands independence of generator.

Swiss Post Public Intrusion Test

Undetectable Attack Against Vote Integrity and Secrecy

1. Manipulation of the Election Result:
   Instead of re-encrypting the shuffled encrypted votes, the malicious mixing component manipulates the input encryption list in an arbitrary way, for example such that the preferred candidate wins the election. Then a fake proof is constructed, which links the manipulated output encryption list to the correct input encryption list. The verification of the proof will succeed and the attack remains undetected.

Solution (FIPS 186-4 and ROCQ)

1: **procedure** VERIFIABLE-GENERATOR-PROCEDURE($p, q, domain\_parameter\_seed, index$)
2: **Result**: *status*, g
3: **if** *index* is incorrect **then** return **INVALID**
4: **end if**
5: $N = \textbf{len}(q)$
6: $k = (p-1)/q$
7: $count = 0$
8: $count = count + 1$
9: **if** $count = 0$ **then** return **INVALID**
10: **end if**
11: $U = domain\_parameter\_seed \,||\, \text{“ggen”} \,||\, index \,||\, count$
12: $W = \textbf{Hash}(U)$
13: $g = W^k \bmod p$
14: **if** $g < 2$ **then**, go to step 8
15: **end if**
16: Return **VALID** and the value of g
17: **end procedure**

ROCQ

A trustworthy, industrial-strength interactive theorem prover and dependently-typed programming language for mechanised reasoning in mathematics, computer science and more.

- Implementation of A.2.3 with a correctness proof that it always produces correct generators.
- Implementation of A.2.4 to validate generators computed according to A.2.3.
- Implementation of the SHA-256 (FIPS 180-4) hash algorithm, required in A.2.3 and A.2.4.
- Implementation of the Fermat's little theorem, needed to prove the correctness of A.2.3 and A.2.4.

```
(* https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf*)
(* Verifiable Canonical Generation of the Generator g  *)
(* Input p, q, and domain_seed *)
(* We assume that that the prime p q has been validated and
   generated by using  domain_parameter_seed *)
Module Type Prime.
  Parameters (p q k domain_parameter_seed ggen index : N).
  Axiom prime_p : prime (Z.of_N p).
  Axiom p_len : 1024 <= N.size p.
  Axiom prime_q : prime (Z.of_N q).
  Axiom q_len : 160 <= N.size q.
  Axiom k_gteq_2 : 2 <= k.
  Axiom safe_prime : p = k * q + 1.
  Axiom ggen_hyp : ggen = 0x6767656e.
  Axiom index_8bit : 0 <= index < 0xff.
End Prime.
```

Instantiate Parameters with Data

```
Module Pins <: Prime.
Definition p : N := (* Prime *)
Definition q : N := (* Prime *)
Definition k : N := Eval vm_compute in N.div (p - 1) q.
Definition domain_parameter_seed : N :=  (* Domain Parameter Seed *)
Definition ggen : N := 0x6767656e.
Definition index : N := (* Index *)
```

Discharge all Axioms

```
Theorem prime_p : prime (Z.of_N p).
(* Discharge the proof *)

Theorem p_len : 1024 <= N.size p.
(* Discharge the proof *)

Theorem prime_q : prime (Z.of_N q).
(* Discharge the proof *)
```

```
Theorem q_len : 160 <= N.size q.
(* Discharge the proof *)

Theorem k_gteq_2 : 2 <= k.
(* Discharge the proof *)

Theorem safe_prime : p = k * q + 1.
(* Discharge the proof *)
```

Construct a Module

```
(* get a concrete instance *)
Module genr := Comp Pins.

(* Call the function *)
Time Eval vm_compute in genr.compute_generator.
```

```
Time Eval vm_compute in genr.compute_generator.


Finished transaction in 1479.475 secs (1478.121u,1.187s) (successful)
= genr.Valid
5142269046611298751053334471712018380952381659994149061069643310780863411117756830385169625171306902268731945265611175832982085711414921325430792621067001642054430322541316695452318115167970016625546426097672467620839422473921709026039725510992923909031023192174059668984872166791847785098121010517945765446961570007177822942898941331888153276962092525360573272974634978013864168046512739478574948414329466141821447534309755925230066981468451347043551719324995849899067726237010049836515585927730058820192474169847466483361570985526862054236113750881396542483192524341448209408531022129289703356623973794545446814225059247328981961060656844942121203760003864474654437004736370165730970677136513883966628087789535547496889264530799006158784007444380513118730444715144566680249530571284451878484157389189765788664403469491470323677756901984779279566477157877271477923138873212496519999904917186456515597600968771835406001603690 : genr.Tag
```

Proof of Correctness

$$g^q \equiv 1 \mod p$$

```
Lemma correct_compute_genertor :
  forall g,  Valid g = compute_generator ->
  Zpow_mod (Z.of_N g) (Z.of_N q) (Z.of_N p) = 1%Z.
Proof.
```

Proof of Correctness

Generation and Verification algorithms agree with each other.

```
Lemma generator_verifier_correctness : forall g,
  verify_generator g = true <-> Valid g = compute_generator.
Proof.
```

Challenge

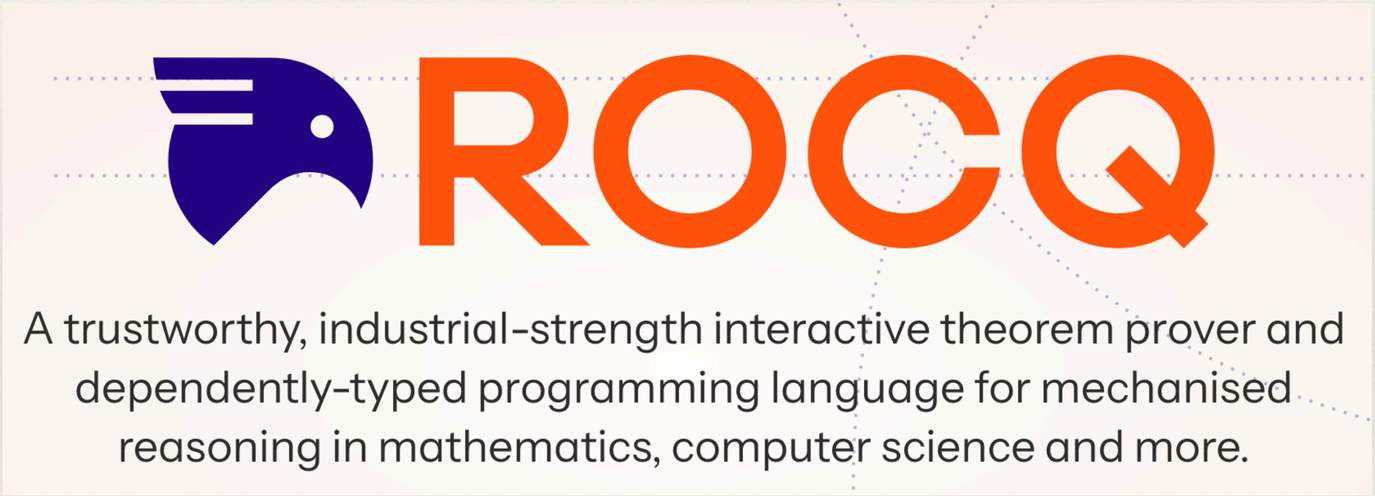
```
Definition sha256_string (s : string) :=
  concat_bytes (List.flat_map big_endien_list_N (sha256 (list_byte_of_string s))).
```

```
Lemma sha256_4th : sha256_string ("abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghij" ++
 "klmnhijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu") =
  0xcf5b16a778af8380036ce59e7b0492370b249b11e8f07a51afac45037afee9d1.
Proof.
  Time vm_compute; reflexivity.
Qed.
```

Evaluation

We use Rocq's evaluation mechanism to compute the group generator, thereby only trusting the Rocq codebase.

- 1 minutes for 1024 bit prime
- 10 minutes for 2048 bit prime
- 30 minutes for 3072 bit prime



```
COQC src/Generator_1.v
Finished transaction in 51.48 secs (51.393u,0.088s) (successful)
     = genr.Valid
         13845410670820047905573533543088887716582050631568180852981258877489129426674596593
     : genr.Tag
```

```
COQC src/Generator_12.v
Finished transaction in 1417.487 secs (1415.836u,1.591s) (successful)
     = genr.Valid
         514226904661129875105333447171201838095238165999414906106964331078086341111775683038
     : genr.Tag
```

Best Part

You do not need to know Rocq to use this software to compute generators!

Conclusion

In this work, we showed how to use the Rocq theorem prover to implement the group generator algorithm (A.2.3), prove its correctness, evaluate it inside the theorem prover itself.

To bootstrap an election, election commission, or any responsible authority, can use our software to produce generators. They just need to publish the Rocq scripts for every generator.

An auditor can audit the claims of the election commission by running the Rocq scripts on their own computer