Comments

- The following invariant is maintained by the algorithm:

$$P_i^*(0) + P_i^*(1) \equiv P_{i-1}^*(r_{i-1}) \bmod q \qquad (8)$$

for $1 \leq i \leq n$.

  - $P_i^*(0) + P_i^*(1)$ equals $\sum_{x_i=0,1} \cdots \sum_{x_n=0,1} \Phi(r_1, \ldots, r_{i-1}, x_i, x_{i+1}, \ldots, x_n)$ modulo q.
  - But the above equals $P_{i-1}^*(r_{i-1}) \bmod q$ by definition.

Comments (concluded)

- The computation of $v_1, v_2, \ldots, v_n$ must rely on Peggy's supplied polynomials as Victor does not have the power to carry out the exponential-time calculations.
- But $\Phi(r_1, r_2, \ldots, r_n)$ in Step 12 is computed without relying on Peggy's polynomials.

Completeness

- Suppose ϕ is unsatisfiable.
- For $i \geq 1$, by Eq. (8) on p. 594,

$$\begin{aligned} & P_i^*(0) + P_i^*(1) \\ = & \sum_{x_i=0,1} \sum_{x_{i+1}=0,1} \cdots \sum_{x_n=0,1} \Phi(r_1, \ldots, r_{i-1}, x_i, x_{i+1}, \ldots, x_n) \\ = & P_{i-1}^*(r_{i-1}) \\ \equiv & v_{i-1} \bmod q. \end{aligned}$$

Completeness (concluded)

- In particular at $i = 1$, because ϕ is unsatisfiable, we have

$$\begin{aligned} P_1^*(0) + P_1^*(1) &= \sum_{x_1=0,1} \cdots \sum_{x_n=0,1} \Phi(x_1, \ldots, x_n) \\ &\equiv v_0 \\ &= 0 \bmod q. \end{aligned}$$

- Finally, $v_n = P_n^*(r_n) = \Phi(r_1, r_2, \ldots, r_n)$.
- Because all the tests by Victor will pass, Victor will accept ϕ.

Soundness

- Suppose ϕ is not unsatisfiable.
- An honest Peggy following the protocol will fail after sending $P_1^*(z)$.
  - $P_1^*(z) = \sum_{x_2=0,1} \cdots \sum_{x_n=0,1} \Phi(z, x_2, \ldots, x_n)$.
  - So $P_1^*(0) + P_1^*(1) = \sum_{x_1=0,1} \sum_{x_2=0,1} \cdots \sum_{x_n=0,1} \Phi(x_1, x_2, \ldots, x_n) \not\equiv v_0 \bmod q$.
  - But $v_0 = 0$.

Soundness (continued)

- We will show that if Peggy is dishonest in one round (by sending a polynomial other than $P_i^*(z)$), then with high probability she must be dishonest in the next round, too.
- In the last round (Step 12), her dishonesty is exposed.

Soundness (continued)

- Let $P_i(z)$ represent the polynomial sent by Peggy in place of $P_i^*(z)$.
- Victor calculates $v_i = P_i(r_i) \bmod p$.
- In order to deceive Victor in the next round, round $i+1$, Peggy must use $r_1, r_2, \ldots, r_i$ to find a $P_{i+1}(z)$ of degree at most m such that

$$P_{i+1}(0) + P_{i+1}(1) = v_i \bmod q$$

  (see Step 8 of the algorithm on p. 593).
- And so on to the end, except that Peggy has no control over Step 12.

A Key Claim

Theorem 88 *If $P_i^*(0) + P_i^*(1) \not\equiv v_{i-1} \bmod q$, then either Victor rejects in the ith round, or $P_i^*(r_i) \not\equiv v_i \bmod q$ with probability at least $1 - (m/q)$, where the probability is taken over Victor's choices of r_i.*

- Remember that Victor has no way of knowing $P_i^*(r_i)$.
- Victor calculates v_i with $P_i(z)$, claimed by the not necessarily trust-worthy Peggy as $P_i^*(z)$.
- So $v_i = P_i(r_i) \bmod q$.
- What Victor can do is to check for consistencies.

The Proof of Theorem 88 (continued)

- If Peggy sends a $P_i(z)$ which equals $P_i^*(z)$, then

$$P_i(0) + P_i(1) = P_i^*(0) + P_i^*(1) \not\equiv v_{i-1} \bmod q,$$

and Victor rejects immediately.

- Suppose Peggy sends a $P_i(z)$ different from $P_i^*(z)$.
- If $P_i(z)$ does not pass Victor's test

$$P_i(0) + P_i(1) \equiv v_{i-1} \bmod q, \qquad (9)$$

then Victor rejects and we are done, too.

The Proof of Theorem 88 (concluded)

- Finally, assume $P_i(z)$ passes the test (9).
- $P_i(z) - P_i^*(z) \not\equiv 0$ is a polynomial of degree at most m.
- Hence equation $P_i(z) - P_i^*(z) \equiv 0 \bmod q$ has at most m roots $r_i \in Z_q$, i.e.,

$$P_i^*(r_i) \equiv v_i \bmod q.$$

- Hence, Victor will pick one of these as his r_i so that

$$P_i^*(r_i) \equiv v_i \bmod q$$

with probability at most m/q.

Soundness (continued)

- Suppose Victor does not reject in any of the first n rounds.
- As ϕ is not unsatisfiable,

$$P_1^*(0) + P_1^*(1) \not\equiv v_0 \bmod q.$$

- By Theorem 88 (p. 601) and the fact that Victor does not reject, we have $P_1^*(r_1) \not\equiv v_1 \bmod q$ with probability at least $1 - (m/q)$.
- Now by Eq. (8) on p. 594,

$$P_1^*(r_1) = P_2^*(0) + P_2^*(1) \not\equiv v_1 \bmod q.$$

Soundness (concluded)

- Iterating on this procedure, we eventually arrive at

$$P_n^*(r_n) \not\equiv v_n \bmod q$$

with probability at least $(1 - m/q)^n$.

- As $P_n^*(r_n) = \Phi(r_1, r_2, \ldots, r_n)$, Victor's last test at Step 12 fails and he rejects.
- Altogether, Victor rejects with probability at least

$$[\,1 - (m/q)\,]^n > 1 - (nm/q) > 2/3$$

because $q > 2^n 3^m$.

An Example

- $(x_1 \lor x_2 \lor x_3) \land (x_1 \lor \neg x_2 \lor \neg x_3)$.
- The above is satisfied by assigning true to x_1.
- The arithmetized formula is

$$\Phi(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \times [\, x_1 + (1 - x_2) + (1 - x_3)\,].$$

- Indeed, $\sum_{x_1=0,1} \sum_{x_2=0,1} \sum_{x_3=0,1} \Phi(x_1, x_2, x_3) = 16 \neq 0$.
- We have $n = 3$ and $m = 2$.
- A prime q that satisfies $q > 2^3 \times 3^2 = 72$ is 73.

An Example (continued)

- The table below is an execution of the algorithm in Z_{73} *when Peggy follows the protocol.*

i	$P_i^*(z)$	$P_i^*(0) + P_i^*(1)$	$= v_{i-1}$?	r_i	v_i
0					0
1	$4z^2 + 8z + 2$	16	no		

- Victor therefore rejects ϕ early on at $i = 1$.

An Example (continued)

- Now suppose Peggy does not follow the protocol.
- In order to deceive Victor, she comes up with fake polynomials $P_i(z)$ from beginning to end.
- The table below is an execution of the algorithm.

i	$P_i(z)$	$P_i(0) + P_i(1)$	$= v_{i-1}$?	r_i	v_i
0					0
1	$8z^2 + 11z + 27$	0	yes	10	61
2	$10z^2 + 9z + 21$	61	yes	4	71
3	$z^2 + 2z + 34$	71	yes	r_3	$P_3(r_3)$

An Example (concluded)

- Victor has been satisfied up to round 3.
- Finally at Step 12, Victor checks if

$$\Phi(10, 4, r_3) \equiv P_3(r_3) \bmod 73.$$

- It can be verified that the only choices of $r_3 \in \{\, 0, 1, \ldots, 72 \,\}$ that can mislead Victor are 10 and 12.
- The probability of that happening is only 2/73.[a]

[a] The calculation is in fact incorrect, as such r_3 do not exist in this case. But you got the idea. Contributed by Ms. Ching-Ju Lin (R92922038) on January 7, 2004.

An Example

- $(x_1 \lor x_2) \land (x_1 \lor \neg x_2) \land (\neg x_1 \lor x_2) \land (\neg x_1 \lor \neg x_2)$.
- The above is unsatisfiable.
- The arithmetized formula is

$$\Phi(x_1, x_2) = (x_1 + x_2) \times (x_1 + 1 - x_2) \times (1 - x_1 + x_2) \times (2 - x_1 - x_2).$$

- Because $\Phi(x_1, x_2) = 0$ for any *boolean* assignment $\{0, 1\}^2$ to (x_1, x_2), certainly

$$\sum_{x_1=0,1} \sum_{x_2=0,1} \Phi(x_1, x_2) = 0.$$

- With $n = 2$ and $m = 4$, a prime q that satisfies $q > 2^2 \times 3^4 = 4 \times 81 = 324$ is 331.

An Example (concluded)

- The table below is an execution of the algorithm in Z_{331}.

i	$P_i^*(z)$	$P_i^*(0) + P_i^*(1)$	$= v_{i-1}$?	r_i	v_i
0					0
1	$z(z+1)(1-z)(2-z)$ $+(z+1)z(2-z)(1-z)$	0	yes	10	283
2	$(10+z) \times (11-z)$ $\times(-9+z) \times (-8-z)$	283	yes	5	46

- Victor calculates $\Phi(10, 5) \equiv 46 \bmod 331$.
- As it equals $v_2 = 46$, Victor accepts ϕ as unsatisfiable.

Objections to the Soundness Proof?[a]

- Based on the steps required of a cheating Peggy on p. 600, why must we go through so many rounds (in fact, n rounds)?
- Why not just go directly to round n:
  - Victor sends $r_1, r_2, \ldots, r_{n-1}$ to Peggy.
  - Peggy returns with a (claimed) $P_n^*(z)$.
  - Victor accepts if and only if $\Phi(r_1, r_2, \ldots, r_{n-1}, r_n) \equiv P_n^*(r_n) \bmod q$ for a random $r_n \in Z_q$.

[a]Contributed by Ms. Emily Hou (D89011) and Mr. Pai-Hsuen Chen (R90008) on January 2, 2002.

Objections to the Soundness Proof? (continued)

- Let us analyze the compressed proposal when ϕ is satisfiable.
- To succeed in foiling Victor, Peggy must find a polynomial $P_n(z)$ of degree m such that

$$\Phi(r_1, r_2, \ldots, r_{n-1}, z) \equiv P_n(z) \bmod q.$$

- But this she is able to do: Just give the verifier the polynomial $\Phi(r_1, r_2, \ldots, r_{n-1}, z)$!
- What has happened?

Objections to the Soundness Proof? (concluded)

- You need the intermediate rounds to "tie" Peggy up with a chain of claims.
- In the original algorithm on p. 593, for example, $P_n(z)$ is bound by the equality $P_n(0) + P_n(1) \equiv v_{n-1} \bmod q$ in Step 8.
- That v_{n-1} is in turn derived by an earlier polynomial $P_{n-1}(z)$, which is in turn bound by $P_{n-1}(0) + P_{n-1}(1) \equiv v_{n-2} \bmod q$, and so on.

Finis