
University of Oxford
Mathematical Institute
2nd Oxford
Post-Quantum Cryptography
Summit 2023
PQ SHIELD
National Cyber Security Centre

2nd Oxford Post-Quantum Cryptography Summit 2023

VOX and PROV

Benoît Cogliati, Jean-Charles Faugère, Pierre-Alain Fouque, Louis Goubin, Robin Larrieu, Gilles Macario-Rat, Brice Minaud, Jacques Patarin

Orange, Thales, Versailles St-Quentin University, Rennes University, CryptoNext

VOX

2nd Oxford
Post-Quantum Cryptography
Summit 2023

- What it is
- How it is made
- How it works
- How nice it is

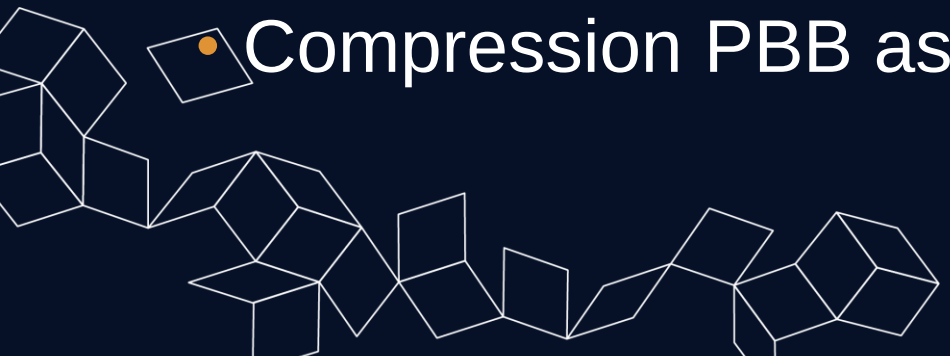
Features of VOX

2nd Oxford Post-Quantum Cryptography Summit 2023

- VOX : like UOV, but better !
- UOV (n=o+v,m=o,q) based
- Hat Plus : t secret equations are set as complete random
- o and v have a common divider l => enables QR transformation
- Public and Secret compression (for free)

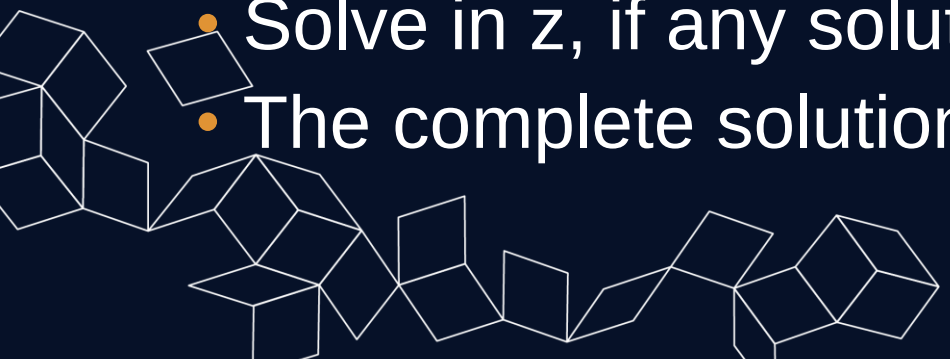
Key Generation

- Generate UOV ($n=o/l+v/l, m=o, q^l$) secret key
  - Note: Min(l)=1 corresponds to plain UOV ; Max(l) = GCD(o,v)
- Complete the last t equations with random coefficients
  - Note Min(t)=0 does nothing ; Max(t)=m is a complete random key
- Add S in Pub = S o Sec o T (S in F_q, T in F_q^l)
- You get: Vox(n=o+v,m=o, q, t, l)
- Compression PBB as with UOV



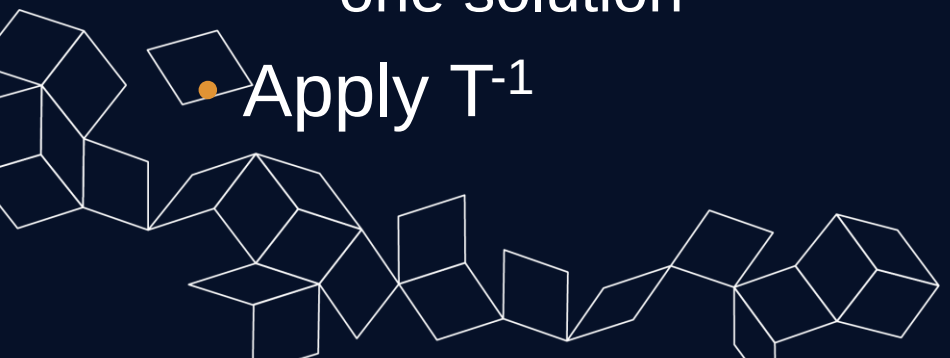
Inversion of the secret map

- Fix vinegar variables with random values : B
- The first o-t equations represent a (o, o-t) - linear system
  - Its solutions can (with great probability) be described as an affine space of dimension t
  - $A = A_0 + z_1 A_1 + \ldots + z_t A_t$ with free variables $z_1, \ldots, z_t$
- Substitute in the last t equations, to get a (t, t) – quadratic system
- Solve in z, if any solution then substitute in A
- The complete solution is then A || B



Signature

- Hash and Sign
- Apply S^{-1}
- Invert the secret map, until a solution is found (≈1.5 times in average)
  - The (o, o-t) linear system has $(1 – 1/q^{t+1})$ probability to be regular
  - The (t, t) quadratic system has ≈ (1 – t/q) to be regular with at least one solution
- Apply T^{-1}

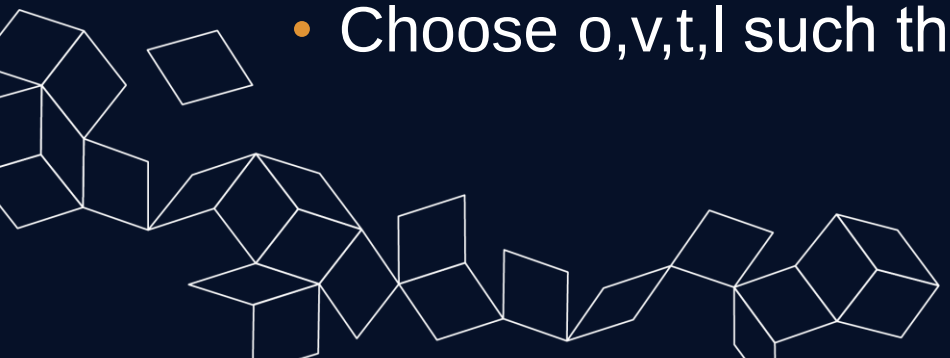


Attacks

- Direct attack
  - Choose parameter against MQ estimator
- Distinguishing attacks (UOV)
  - Choose $q^{3t} \geq 2^{\lambda}$
- Structural attacks : Rectangular MinRank attack

(pqc forum : Comment from Hiroki Furue)

  - Choose o,v,t,l such that Min(o, v/l + t) ≥ Min (o, v/l + o/l) (i.e. t ≥ o/l)



Performance

2nd Oxford Post-Quantum Cryptography Summit 2023

- Example Level I
- q = 251
- o/l = 6
- v/l = 7
- t = 6
- l = 8

- |SIG| = 104 B
- |PK| = 7,088 B
- |SK| = 27,952
- KeyGen = 390 µs
- Sign = 270 µs
- Verify = 20 µs

Features of Prov

2nd Oxford Post-Quantum Cryptography Summit 2023

- UOV based
- δ equations are removed
- Salted
- BUFF tweak
- Public and Secret key compression (for free)
- Main objective : Security proof !

Inversion of the secret map

2nd Oxford Post-Quantum Cryptography Summit 2023

- With high probability, the (o,o-δ) linear system is regular, hence it has q^{δ} solutions.
- The signatures are (almost) uniformly distributed.

Signature

- The signature is a solution in x of
  - Pub(x) = Hash(Hpk || message || salt)
- Hpk is a hash of the public key (BUFF tweak)
- Vinegar is drawn at random only once
- Salt is drawn at random until the derived linear system has a solution

Security of Signature

2nd Oxford Post-Quantum Cryptography Summit 2023

- The property of EUF-CMA of PROV can be proven in both classical and Quantum random Oracle Model, provided the problem on inverting PROV is hard.

Performance

2nd Oxford Post-Quantum Cryptography Summit 2023

- Example Level I
- q = 256
- n = o + v = 136
- m = o – δ = 46
- δ = 8

- |SIG| = 160 B
- |PK| = 68,326 B
- |SK| = 203,752 B

2nd Oxford
Post-Quantum
Cryptography
Summit 2023

Sites

- http://vox-sign.com
- http://prov-sign.github.io

- Thank You !

- Dankon !

2nd Oxford
Post-Quantum Cryptography
Summit 2023