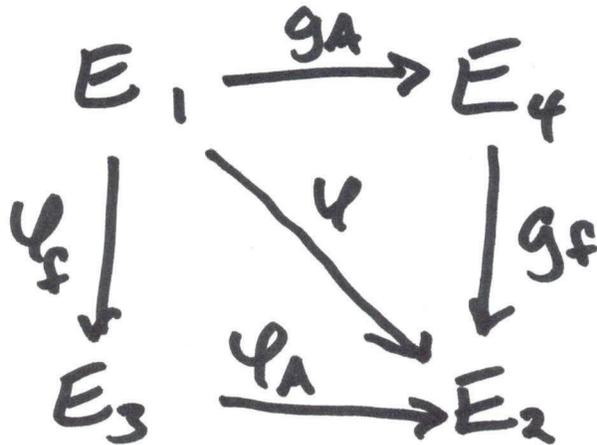


Applying "HD Representations"

Kani's Reducibility Criterion

$f \circ A = B$



$\Phi : E_1 \times E_2 \rightarrow E_3 \times E_4$

$\begin{pmatrix} \phi_f & -\hat{\phi}_A \\ g_A & \hat{g}_f \end{pmatrix}$

$\ker \Phi = \{ ([A]P, \phi(P)) : P \in E, [B] \}$

Denote $\phi|_B = (\phi(P), \phi(Q))$

where $E, [B] = \langle P, Q \rangle$

SQ Sign 2D - West De Feo -

13-2

Dartois - Leroux - Maino - Pope - Robert
Wesolowski

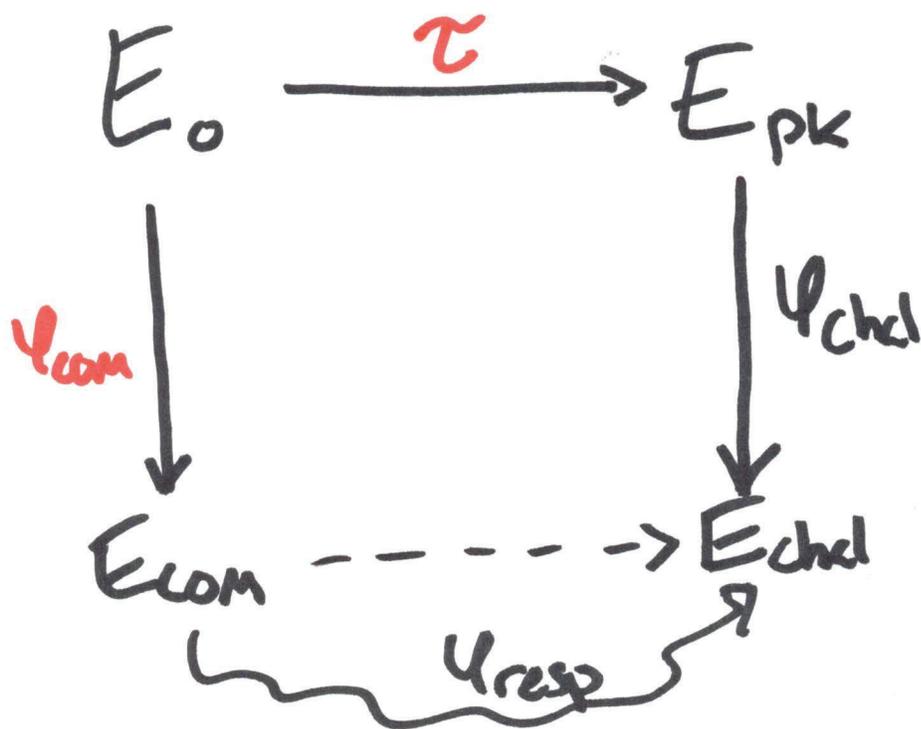
Benefit: uses 2-dim abelian var.
and still has guaranteed sol'n to
relevant equations.

Still a Fiat-Shamir transform
of a Σ -protocol.

Public Parameters:

E_0 : supersingular

$\text{End}(E_0)$ is known.



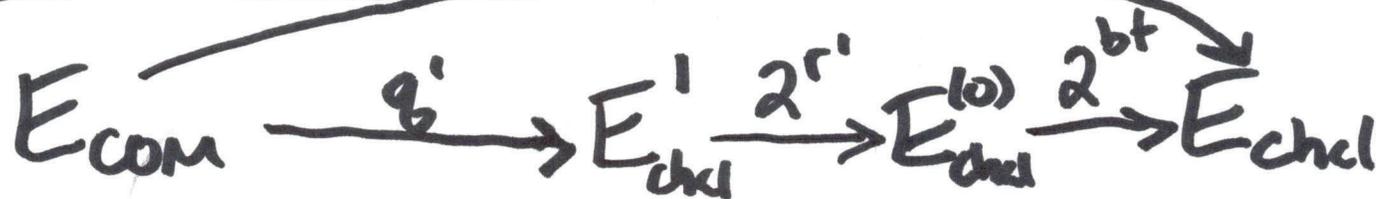
(P) Commitment: $\psi_{com}: E_0 \rightarrow E_{com}$
 stored as ~~commitment~~ $\psi_{com}/2$

(V) Challenge: $E_{pk}[2^c] = \langle P_{pk}, Q_{pk} \rangle$
 $\deg \psi_{chal} = 2^c$ $\ker \psi_{chal} = \langle P_{pk} + [c]Q_{pk} \rangle$
 communicated via "c".

(P) Respond w/ $\psi_{resp}: E_{com} \rightarrow E_{chal}$

Response

(34)



$$1) \# (\ker \hat{\Psi}_{chcl} \cap \ker \hat{\Psi}_{resp}) = 2^{bt}$$

$$2) \deg \Psi_{resp} = g' \underset{\uparrow}{2^{r'}} 2^{bt} \quad \text{w/ } g' \text{ odd}$$

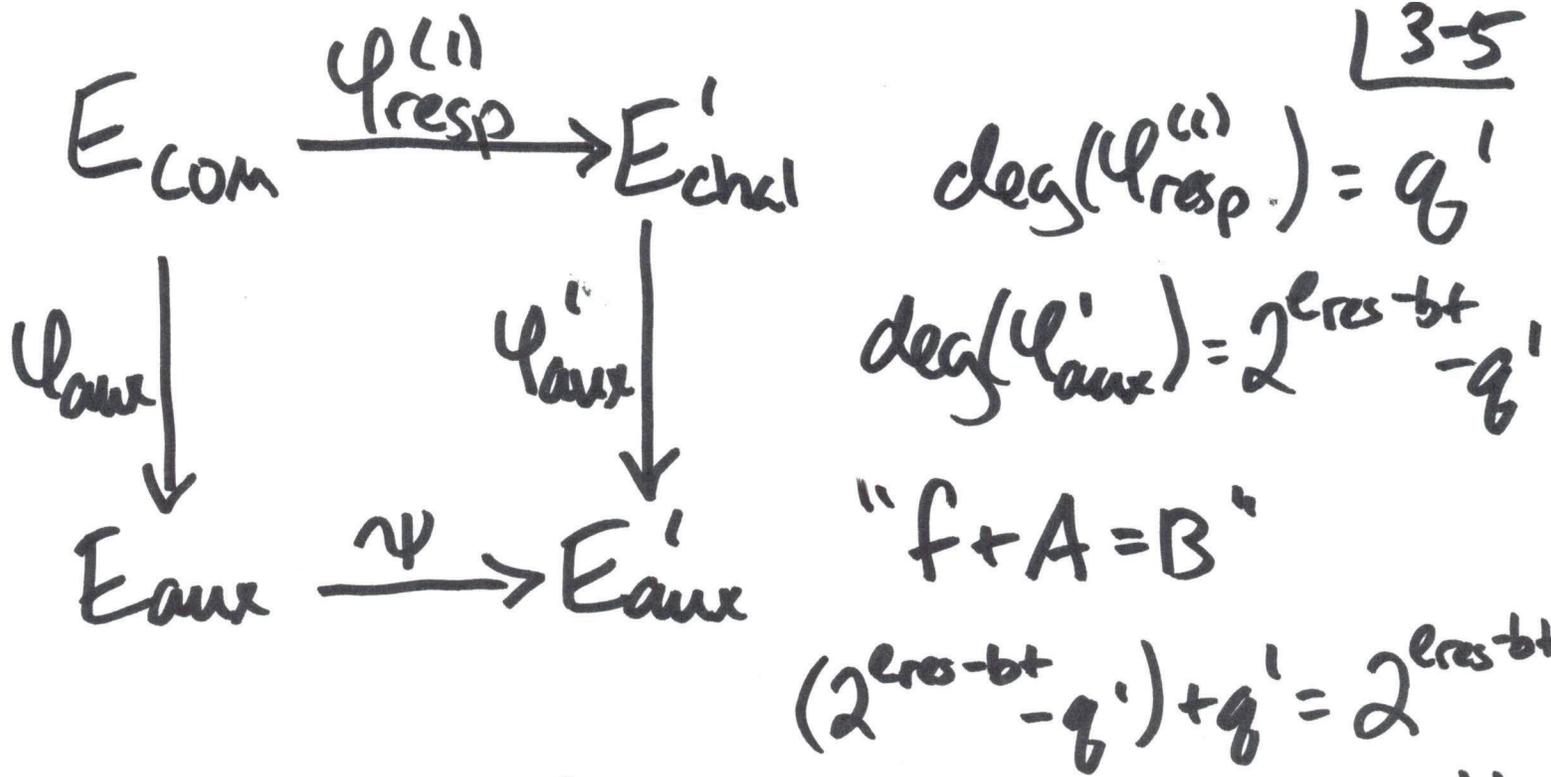
deg-2-power part not backtracking

$$3) \Psi_{resp}^{(1)} : E_{com} \rightarrow E'_{chcl}$$

deg = g' odd has an efficient representation.

For clarity, suppose $r' = 0$

$$\Psi_{resp} = \Psi_{resp}^{bt} \circ \Psi_{resp}^{(1)}$$



$$\Phi : E_{\text{com}} \times E'_{\text{aux}} \rightarrow E_{\text{aux}} \times E'_{\text{chcl}}$$

$$\begin{pmatrix} \psi_{\text{aux}} & \hat{\psi} \\ \psi^{(1)}_{\text{resp}} & \hat{\psi}'_{\text{aux}} \end{pmatrix}$$

$$\text{w/ } \ker \Phi = \left\{ ([q']P, \underbrace{\psi'_{\text{aux}} \circ \psi^{(1)}_{\text{resp}}(P)}_{P \in E_{\text{com}}[2^{\text{eres} - \text{bt}}]}) : \right.$$

$$\begin{array}{l}
 \text{Encode as} \\
 (\psi'_{\text{aux}} \circ \psi^{(1)}_{\text{resp}}(P), \psi'_{\text{aux}} \circ \psi^{(1)}_{\text{resp}}(Q))
 \end{array}$$

↑ Basis

Verification

13-6

- ψ_{chd} from "[C]" challenged
 - Prove correctness of ψ_{resp} in pieces according to q', r' , but using Kani computations.
-

Security

Complete: honest verifier is convinced by an honest prover

Sound: Dishonest prover cannot convince a verifier.

Zero-knowledge: verifier learns nothing about the τ isogeny through this interaction.

Fiat-Shamir Transform

13-7

→ Remove interaction to obtain a digital signature:

Signer: pk, sk

To sign a document D ,
produce a signature $(D, \underline{D + sk})$
which can be verified with
"pk".

Prover (now "signer") compute transcripts $(\psi_{com}, \psi_{chcl}, \psi_{resp})$

where $\psi_{chcl} = H(\psi_{com}, pk, D)$

The verifier looks at several transcripts to verify the signature.

Security Improvements + Efficiency (3-8)

1) The response isogeny degree has no smoothness conditions.

More random + smaller.

2) Doesn't require isogenies in dimension > 2 .

3) Verification is faster

→ Faster + smaller! spisign.org

NIST-I: $p = 5 \cdot 2^{248} - 1$

pk: 65 bytes

sign: 148 bytes

(Optimized) keygen: 43.3 megacycles
signing: 101.6
verifying: 5.1