Arpin + Martindale - Lecture III
Applying "HD Representations"

Kani's Reducibility Criterion

$f + A = B$

$$\begin{tikzcd} E_1 \arrow[r, "g_A"] \arrow[d, "\varphi_f"'] \arrow[dr, "\varphi"] & E_4 \arrow[d, "g_f"] \\ E_3 \arrow[r, "\varphi_A"] & E_2 \end{tikzcd}$$

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

$$\begin{pmatrix} \varphi_f & -\hat{\varphi}_A \\ g_A & \hat{g}_f \end{pmatrix} \qquad \ker \Phi = \{([A]P, \varphi(P)) : P \in E_1[B]\}$$

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

where $E_1[B] = \langle P, Q \rangle$

SQIsign2D-West De Feo-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

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

$$
\begin{tikzcd}
E_0 \arrow[r, "\tau"] \arrow[d, "\varphi_{com}"'] & E_{pk} \arrow[d, "\varphi_{chl}"] \\
E_{com} \arrow[r, dashed] \arrow[r, bend right, squiggly, "\varphi_{resp}"'] & E_{chl}
\end{tikzcd}
$$

(P) Commitment: $\varphi_{com} : E_0 \to E_{com}$
stored as $\varphi_{com}|_2$

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

(P) Respond w/ $\varphi_{resp} : E_{com} \to E_{chl}$

Response

$$\begin{tikzcd} E_{com} \arrow[r, "q'"] \arrow[rrr, bend left, "\varphi_{resp}"] & E'_{chal} \arrow[r, "2^{r'}"] & E^{(0)}_{chal} \arrow[r, "2^{bt}"] & E_{chal} \end{tikzcd}$$

1) $\#\left(\ker \hat{\varphi}_{chal} \cap \ker \hat{\varphi}_{res}\right) = 2^{bt}$

2) $\deg \varphi_{resp} = q' 2^{r'} 2^{bt}$ w/ q' odd

deg-2-power part not backtracking

3) $\varphi^{(1)}_{res} : E_{com} \to E'_{chal}$

deg $= q'$ odd has an efficient representation.

For clarity, suppose $r' = 0$

$$\varphi_{resp} = \varphi^{bt}_{resp} \circ \varphi^{(1)}_{resp}$$

$$
\begin{tikzcd}
E_{com} \arrow[r, "\varphi^{(1)}_{resp}"] \arrow[d, "\varphi_{aux}"'] & E'_{chal} \arrow[d, "\varphi'_{aux}"'] \\
E_{aux} \arrow[r, "\psi"] & E'_{aux}
\end{tikzcd}
$$

$$\deg(\varphi^{(1)}_{resp}) = q'$$

$$\deg(\varphi'_{aux}) = 2^{e_{res}-bt} - q'$$

"$f + A = B$"

$$(2^{e_{res}-bt} - q') + q' = 2^{e_{res}-bt}$$

$$\Phi : E_{com} \times E'_{aux} \to E_{aux} \times E'_{chal}$$

$$\begin{pmatrix} \varphi_{aux} & -\hat{\psi} \\ \varphi^{(1)}_{resp} & \hat{\varphi}'_{aux} \end{pmatrix}$$

w/

$$\ker \Phi = \left\{ \left([q']P, \underline{\varphi'_{aux} \circ \varphi^{(1)}_{resp}}(P) \right) : P \in E_{com}[2^{e_{resp}-bt}] \right\}$$

Basis

Encode as

$$\left(\varphi'_{aux} \circ \varphi^{(1)}_{resp}(P), \varphi'_{aux} \circ \varphi^{(1)}_{resp}(Q) \right)$$

Verification

- φ_{chal} from "[c]" challenged
- Prove correctness of φ_{resp}

in pieces according to q', r', b' using Kani computations.

Security

Compete: 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

→ Remove interaction to obtain a <u>digital signature</u>:

Signer: pk, sk

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

Prover (now "signer") compute transcripts (φ_{com}, φ_{chal}, φ_{resp}) where $\varphi_{chal} = H(\varphi_{com}, pk, D)$

The verifier looks at several transcripts to verify the signature.

Security Improvements + Efficiency

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!

sqisign.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 " "