Matthew Townsend

CS 522 Networks

A Note on Hybrid Signature Schemes

The need for hybridization is driven by a conundrum: the pressing need to adopt Post Quantum algorithms, coupled with the awareness of potential, hidden subtleties in their security. While standard algorithms like RSA are based on well-understood factoring hardness assumptions, many PQ algorithms rely on more complex assumptions that have not undergone pervasive cryptanalysis.

Complex PQ algorithms, such as CRYSTALS-Dilithium, are supported by extensive specifications, contrasting with the relative simplicity of RSA . The failure of algorithms like SIKE(see summary 4, a lot of math) during the NIST competition serves as a warning that more cryptanalysis is necessary, but time for delay is scarce. Hybrid algorithms offer a path forward by combining the security properties of standard and PQ algorithms.

Hybridization for digital signatures is more subtle than for key encapsulation methods because the verification tag must attest to both components, risking downgrading attacks or separability. The primary design goals examined:

1. Proof Composability: The security of the hybrid signature must be easily reducible to the component algorithms (standard and PQ).

2. Non-Separability: The guarantee that an adversary cannot simply remove either the standard or PQ digital signature component. This exists on a spectrum:

◦ Weak Non-Separability (WNS): Artifacts remain if a signature is stripped, potentially outside the signature. WNS allows for a valid separation under leftover artifacts.

◦ Strong Non-Separability (SNS): Separation causes verification to fail entirely; an adversary cannot produce a valid partial signature. This aligns more closely with traditional digital signature security experiments (EUF-CMA).

◦ Note on Compatibility: There is an inherent mutual exclusion between backwards compatibility and SNS. Backwards compatibility allows a legacy receiver to verify only the standard component.

3. Simultaneous Verification (SV): An extension of SNS and a core focus of this work, requiring that both standard and PQ component verifications succeed simultaneously. SV ensures that the verifier cannot terminate the process with a successful verification of only one component, mirroring traditional digital signature guarantees.

4. Hybrid Generality: Constructions should be based on common structures, allowing for plug-and-play instances with different algorithms.

Seems Legit: Automated Analysis of Subtle Attacks on Protocols That Use Signatures

EUF-CMA security allows for subtle behaviours, including the possibility that one signature may verify against multiple distinct public keys, or that an adversary can: Generate a new key pair that verifies an existing signature, Change parts of a signature without affecting its validity, and Compute weak keypairs where a single signature verifies against multiple messages

To address this shortcoming, the authors introduce a new hierarchy of tool-agnostic symbolic models for digital signatures:

1. Falsification Models (Attack Finding): These models capture specific subtle behaviours omitted from traditional models, enabling the automatic discovery of attacks. They model the absence of properties such as Conservative Exclusive Ownership , Destructive Exclusive Ownership, non-malleability, non-resign-ability, and non-collidability.

- The no-CEO model, for instance, allows an adversary, given a valid signature, to construct a new public key against which the signature also verifies.
- The Malleability model extends the signature term to include a malleable part, allowing the adversary to modify a signature while keeping it valid for the same message and key.

2. Symbolic Verification of Signatures (SVS) Model: For robust verification, a general model was developed that adheres closely to the computational security definition, making minimal assumptions. The SVS model specifies constraints based only on EUF-CMA: verification must succeed for correct, honest signatures (Correctness), and fail for forged signatures against honest keys (NoForgery). Finally, for all other cases the adversary can choose the verification outcome, thereby implicitly allowing key substitution, colliding signatures, and other unknown behaviors unless they violate the computational definition.

Protocol Variant	Previous Analysis Model	Property Violated	Attack Signature Property	Reference
WS-Security X.509 Mutual Auth	Traditional Symbolic Model	Correlation & Secrecy	No-CEO (Key Substitution)	New finding
DRKey Key Exchange Protocol	Coq Proof	Authentication & Collusion-Resistance	Re-sign/Colliding Signatures	New finding
ACME Draft 00 (Let's Encrypt)	Traditional Symbolic Model	DNS Validation	No-DEO (Key Substitution)	Confirmed known attack
STS-MAC (Original)	Traditional Symbolic Model	Identity Agreement	No-CEO	Confirmed known attack

BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures

1. Exclusive Ownership (EO): The property that a signature only verifies under a single public key. The strongest variant formalized is Malicious-Strong Universal Exclusive Ownership (M-S-UEO). A lack of this property allows an attacker to construct a new key pair under which an existing valid signature also verifies, potentially leading to key substitution attacks (DSKS).

2. Message-Bound Signatures (MBS): The property that a signature is valid for a unique message. Its absence can lead to problems in protocols that depend on uniqueness, especially in the presence of adversarially chosen keys, as seen in schemes like DSA and ECDSA.

3. Non Re-signability (NR): The inability to produce a valid signature under another key given a signature for some unknown message m. This is crucial because standard schemes like RSA allow producing a new signature without knowing the original message m. This paper provides the first formal cryptographic definition for NR.

The BUFF Transformation

To efficiently achieve these necessary protections, the authors introduce a simple, generic transformation called BUFF (Beyond UnForgeability Features).

- Goal and Achievement: The BUFF transformation takes any EUF-CMA-secure signature scheme and transforms it into a scheme that provably achieves M-S-UEO, MBS, and NR simultaneously. This protection holds even in the presence of weak keys.

- Mechanism: BUFF builds on previous work, modifying the signature process so that the signature is derived from the hash of the message concatenated with the public key, and the resulting signature includes the computed hash digest, H(m,pk), appended to the original signature, Sig(sk,H(m,pk)).

- Efficiency: The transformation is highly efficient, relying on the hash function H being collision resistant and Φ-non-malleable. It only increases the size of the signature moderately by a single hash digest. For schemes where the required hash value already appears as part of the signature (like Fiat-Shamir schemes), the transformation incurs no size or computational penalty.

Scheme	M-S-UEO	MBS	NR	Conclusion
CRYSTALS-Dilithium	3	3	3	All properties hold.
FALCON	7	3	7	Fails M-S-UEO (S-CEO) and NR.
Rainbow Standard	7	3	7	Fails M-S-UEO (S-CEO) and NR.
Picnic	3	3	3	All properties hold.
GeMSS	7	7	7	Fails all three properties.
SPHINCS+	·	3	·	MBS holds; others intuitively expected but not formally proven under standard assumptions.

Fortunately, applying the BUFF transformation to the vulnerable PQC schemes can efficiently remedy these security gaps, making them harder to misuse. The cost of applying BUFF to these schemes is minimal

Efficient Key Recovery Attack on SIDH

The attack, presented by Wouter Castryck and Thomas Decru of imec-COSIC, KU Leuven, cracks SIKE, which had advanced to the fourth round of NIST's post-quantum cryptography standardization process.

The attack is considered devastating due to its speed and practicality. It achieves key recovery using classical computation and, assuming knowledge of the starting curve's endomorphism ring, operates in time that is polynomial in the input size (heuristically).

1. Exploitation of Torsion Points: The attack critically relies on the torsion point images that Alice and Bob exchange during the protocol. The target is Bob's secret $3b$-isogeny $\phi{:}Estart{\to}E$. Bob's public key includes the codomain curve E and the image points $P{=}\phi(P0)$ and $Q{=}\phi(Q0)$ of $2a$-torsion points $P0,Q0$.

2. Decision Tool: The core idea is to use Kani's criterion as a decision tool in a search-to-decision reduction algorithm. The criterion tests whether an isogeny emanating from a product of two elliptic curves lands again on a product of elliptic curves.

3. Auxiliary Isogeny (γ): An auxiliary isogeny $\gamma{:}Estart{\to}C$ of degree $c{=}2a{-}3b$ is computed. If the exchanged public key components are valid, a specific $(2a,2a)$-isogeny constructed from $C{\times}E$ using γ and the torsion images must be reducible, meaning it lands on a product of elliptic curves. If the key is invalid, this outcome is extremely unlikely.

4. Efficiency via Richelot Isogenies: Constructing γ relies on factoring $c{=}2a{-}3b$. For SIKE, the starting curves ($Estart$) possess a non-scalar endomorphism $2i$ such that $2i{\circ}2i{=}[-4]$, which simplifies the construction of γ. Once γ is found, the decision algorithm requires computing a chain of (2,2)-isogenies, which is performed very efficiently using Richelot isogenies between Jacobians of genus 2 curves. The final check for reducibility is a simple "$\delta{=}0$ test".

SIKE Parameter Set	NIST Security Level	Approximate Time (Single Core, Magma)
SIKEp434	1	~10 minutes
SIKEp503	2	~20 minutes
SIKEp610	3	~55 minutes
SIKEp751	5	~3 hours 15 minutes