



(Red)ETA: Refreshable Extensible DLOG Enhanced Threshold Algorithms

Alessandro Barenghi¹, Michele Battagliola², Riccardo Longo³,
Alessio Meneghetti⁴, Gerardo Pelosi¹, Edoardo Signorini⁵

1. Polytechnic University of Milan, IT
2. Marche Polytechnic University, IT
3. Fondazione Bruno Kessler, IT
4. University of Bari Aldo Moro, IT
5. Telsy SpA, IT

NIST Workshop on Multi-Party Threshold Schemes 2026
January 26-29 2026



UNIVERSITÀ
POLITECNICA
DELLE MARCHE



Outline of the Talk

Submission Preview

Decentralized Key Generation

Schnorr

EdDSA

ECDSA

(Red)ETA Submission Preview

- ▶ DKG: N4.1
- ▶ Schnorr: N1.1
- ▶ EdDSA: N1.1 + Gadget
- ▶ ECDSA: N1.2

Outline of the Talk

Submission Preview

Decentralized Key Generation

Schnorr

EdDSA

ECDSA

η -DKG (N4.1): Main Properties

- ▶ Decentralized secret generation;
- ▶ Verifiable correctness and coherence of shares;
- ▶ Extensibility: parties may join later on, aided by any authorized subset of users;
- ▶ Refreshability: proactively restore security after partial compromise;
- ▶ Fine-grained access control: compatibility with general access structures (threshold trees).

η -DKG: Components

- ▶ Homomorphic Commitment Scheme: Pedersen commitment;
- ▶ Exploit linear MDS codes and Monotone Span Programs.

η -DKG (N4.1): Security

- ▶ Adaptive Adversary: can react and adapt strategy;
- ▶ Mobile Adversary: can move between parties;
- ▶ Snapshot Adversary: compromises at specific times, not continuous.

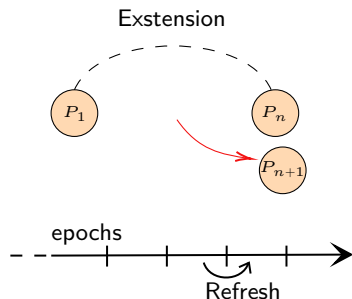
Assumption: DLOG, which gives binding of Pedersen commitment.
References:[1],[2].

[1] Michele Battagliola, Riccardo Longo **and** Alessio Meneghetti. “Extensible decentralized secret sharing and application to Schnorr signatures”. *in* *Designs, Codes and Cryptography*: 94.1 (2025). ISSN: 1573-7586. DOI: 10.1007/s10623-025-01746-1. Also at ia.cr/2022/1551.

[2] Riccardo Longo, Alessio Meneghetti **and** Sara Montanari. *Tighter Control for Distributed Key Generation: Share Refreshing and Expressive Reconstruction Policies*. Cryptology ePrint Archive, Paper 2025/277. 2025. URL: <https://eprint.iacr.org/2025/277>.

η -DKG: Protocol Overview

<u>Keygen₁(J)</u>	<u>Keygen₂(J, {C_{j,k}}_{j∈J})</u>	<u>Keygen₃(J, {β_{j,i}, γ_{j,i}}_{j∈J})</u>
1: $M \leftarrow \text{ConvertPolicy}$	1: $\beta_{i,j} \leftarrow \vec{p}_i M_j$	1: $\text{Hcom}(\beta_{j,i}; \gamma_{j,i}) \stackrel{?}{=} \prod_k (C_{j,k})^{M_{k,i}}$
2: $\vec{p}_i, \vec{z}_i \leftarrow \$_Z_q^{ M }$	2: $\gamma_{i,j} \leftarrow \vec{z}_i M_j$	2: $\beta_i \leftarrow \sum_j \beta_{j,i}$
3: $C_{i,k} \leftarrow \text{Hcom}(p_{i,k}, z_{i,k})$	3: $\text{send}_j(\beta_{i,j}, \gamma_{i,j})$	3: $\gamma_i \leftarrow \sum_j \gamma_{j,i}$
4: $\text{publish}(C_{i,k})$		



Outline of the Talk

Submission Preview

Decentralized Key Generation

Schnorr

EdDSA

ECDSA

η -Schnorr (N1.1): Main Properties

- ▶ Key generation inherited by η -DKG;
- ▶ Threshold Signing: any authorized set can generate a signature
 - ▶ compatible with more general access structures
- ▶ Verification compatible with standard Schnorr

η -Schnorr: Security

- ▶ Static Adversary present since key generation (only DDH+ROM required);
- ▶ Adaptive Adversary if not involved during key generation;
- ▶ Under investigation: security against a Mobile Adversary;

References:[3],[4].

[3] Michele Battagliola, Alessio Galli, Riccardo Longo **and** Alessio Meneghetti. “A provably-unforgeable threshold Schnorr signature with an offline recovery party”. *in* *Ceur Workshop Proceedings: volume 3166*. CEUR-WS. org. 2022, pages 60–76. URL: <https://ceur-ws.org/Vol-3166/paper05.pdf>.

[4] Michele Battagliola, Riccardo Longo **and** Alessio Meneghetti. “Extensible decentralized secret sharing and application to Schnorr signatures”. *in* *Designs, Codes and Cryptography*. 94.1 (2025). ISSN: 1573-7586. DOI: 10.1007/s10623-025-01746-1. Also at ia.cr/2022/1551.

η -Schnorr: Protocol Overview

$\text{Sign}_1(J)$	$\text{Sign}_3(m, J, \{d_j^{r_j}\}_{j \in J})$	$\text{Combine}(m, J, \{d_j^{s_j}\}_{j \in J})$
<pre>1: $k_i \leftarrow \mathbb{Z}_q$ 2: $r_i \leftarrow g^{k_i}$ 3: $(c_i^{r_i}, d_i^{r_i}) \leftarrow \text{Com}(r_i)$ 4: send($c_i^{r_i}$)</pre>	<pre>1: for j in J 2: Open($c_j^{r_j}, d_j^{r_j}$) 3: $r \leftarrow \prod_j r_j$ 4: $\lambda_i \leftarrow \text{Lagrange}(J, i)$ 5: $e \leftarrow H(r \ m)$ 6: $s_i \leftarrow k_i - \lambda_i \cdot e \cdot \text{sk}_i$ 7: send(s_i)</pre>	<pre>1: $s \leftarrow \sum_{j \in J} s_j$ 2: $r \leftarrow g^s \cdot \text{pk}^e$ 3: if $H(r \ m) \neq e$ 4: then abort 5: return (r, s)</pre>
<pre>$\text{Sign}_2(J, \{c_j^{r_j}\}_{j \in J})$ 1: send($d_i^{r_i}$)</pre>		

Outline of the Talk

Submission Preview

Decentralized Key Generation

Schnorr

EdDSA

ECDSA

η -EdDSA (N1.1): Main Properties

Definition (Threshold EdDSA)

Schnorr-like threshold signature where the **deterministic** nonce generation is **verifiable** by the other signers.

- ▶ Signing flexibility inherited from η -Schnorr
- ▶ Verifiable deterministic nonce generation
- ▶ Verification compatible with standard EdDSA

η -EdDSA: Components

- ▶ Elliptic-Curve-based Pseudo-Random Function (PRF) Purify for the verifiable deterministic nonce generation;

Remark

This is not the same PRG defined in standard EdDSA, because SHA-512 has poor compatibility with threshold MPC.

This verifiable deterministic nonce generation may become a **gadget**, interoperable with other Threshold Schnorr protocols.

- ▶ Extra "key-pair" generated with DKG.
- ▶ 1 extra round to compute and verify shares of deterministic nonce.

η -EdDSA: Security

- ▶ Static Adversary present since key generation;
- ▶ Under investigation: security against a adaptive and mobile adversaries;

Assumptions: DDH + ROM.

References:[5].

[5] Michele Battagliola, Riccardo Longo, Alessio Meneghetti **and** Massimiliano Sala. “Provably Unforgeable Threshold EdDSA with an Offline Participant and Trustless Setup”. in *Mediterranean Journal of Mathematics*: 20.5 (june 2023). ISSN: 1660-5454. DOI: 10.1007/s00009-023-02452-9. Also at https://iris.unitn.it/retrieve/handle/11572/384212/660585/BLMS_eddsa.pdf.

Outline of the Talk

Submission Preview

Decentralized Key Generation

Schnorr

EdDSA

ECDSA

η -ECDSA (N1.2): Main Properties

- ▶ Key generation inherited by η -DKG;
- ▶ Threshold Signing: any authorized set can generate a signature
 - ▶ compatible with more general access structures
- ▶ Verification compatible with standard ECDSA

η -ECDSA: Components & Security

Main sub-component:

- ▶ Paillier cryptosystem used during threshold signature generation (multiplicative-to-additive share conversion).

Security:

- ▶ Static Adversary present since key generation;
- ▶ Under investigation: security against a adaptive and mobile adversaries;

Assumptions: DDH + ROM + Strong RSA (for Paillier).

References:[6].

[6] Michele Battagliola, Riccardo Longo, Alessio Meneghetti **and** Massimiliano Sala. “Threshold ECDSA with an Offline Recovery Party”. *in Mediterranean Journal of Mathematics*: 19.1 (**november** 2021). ISSN: 1660-5454. DOI: 10.1007/s00009-021-01886-3. Also at arXiv:2007.04036.

Conclusion

Package contents:

- ▶ DKG (N4.1)
- ▶ Schnorr (N1.1)
- ▶ EdDSA (N1.1+)
- ▶ ECDSA (N1.2)

Main features:

- ▶ Extensibility to later-joining parties
- ▶ Refreshability for proactive security
- ▶ Tighter access control with threshold trees
- ▶ Verifiable deterministic nonces for EdDSA

Thanks for your attention! Any question?

`team@eta-project.org`



UNIVERSITÀ
POLITECNICA
DELLE MARCHE



UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

Telsy
A TM ENTERPRISE BRAND