"Preview Writeup": In anticipation of a package submission to the NIST Threshold Call

Title: Two-Party ECDSA Signatures

Subtitle: Fireblocks's BAM Protocol

Version: 1.0 (2026-01-15)[1]

Team name: Fireblocks–3MI Labs

Team members: Michael Adjedj, Tomer Ashur, Amit Singh Bhati, Geoffroy Couteau, Cyprien Delpech de Saint Guilhem, Michael Gutkin, Nikos Makriyannis

Abstract: This preview write-up presents the plan to submit Fireblocks's *BAM* protocol for two-party ECDSA signature computation. The submission package will also include contents on secret-sharing, Paillier homomorphic encryption, Damgård–Fujisaki and Pedersen commitment schemes, a protocol for vector oblivious linear evaluation, as well as several related zero-knowledge proofs.

Proposed crypto-systems: (I) BAM: Two-Party ECDSA Signing (Categories N1.2 and N4); (II) BAM-Stateless: BAM with Clonable Server Parties (Categories N1.2 and N4).

Keywords: Threshold Cryptography; NIST Threshold Call; ECDSA Key Generation; ECDSA Signature; Identifiable Abort

[1] Version submitted to NIST-MPTC for publication

Preview writeup. This document is provided to NIST for online publication, to foster public awareness and support public discussion within the scope of the NIST First Call for Multi-Party Threshold Schemes [NIST-IR8214C]. This "preview writeup" represents a good-faith plan for a subsequent "package submission". However, until the deadline for package submission, the team may still modify its own composition and the submission plan, including possible changes to the technical scope, and/or the used techniques or achieved results.

Team members: Michael Adjedj [i1,a1], Tomer Ashur [i2,a2], Amit Singh Bhati [i3,a2], Geoffroy Couteau [i4,a3*], Cyprien Delpech de Saint Guilhem [i5,a2], Michael Gutkin [i6,a1], Nikos Makriyannis [i7,a1]

Open Researcher and Contributor Identifiers (ORCID):

i1 (0009-0001-2738-9728); i2 (0000-0001-6091-4857); i3 (0000-0003-0843-4885); i4 (0000-0002-6645-0106); i5 (0000-0002-0147-2566); i6 (0009-0002-5533-7420); i7 (0000-0002-9818-456X)

Affiliations:

[a1] Fireblocks, New York City, NY, United States of America

[a2] 3MI Labs, Leuven, Belgium

[a3] Université Paris Diderot, Paris, France

Associateship clarifications:

[*] Consultant at Fireblocks Ltd.

Main contacts:

- **Team mailing list:** NIST-MPTC@fireblocks.com
- **Primary technical contact person:** Nikos Makriyannis, nikos@fireblocks.com
- **Secondary contact person 1:** Michael Gutkin, gutkin@fireblocks.com
- **Secondary contact person 2:** Cyprien Delpech de Saint Guilhem, cyprien@3milabs.tech

Produced by humans. The team hereby confirms that the content in this preview writeup: (i) was produced by the team members, and (ii) was not produced by generative artificial intelligence (AI), with the possible exception of AI-proposed grammar improvements, minor integrated suggestions, or some well-identified and short localized portions of auxiliary content (e.g., some illustration); and (iii) was proofread by the team members.

1. Introduction

Principal Crypto-Systems. The planned package submission will specify a family of two-party distributed signature crypto-systems for the ECDSA signature scheme based on Fireblock's *BAM protocol* [ABCGJM24]. This family fits within categories N1.2 (ECDSA signing) and N4 (subcategory QV-ECC-KeyGen). We also intend to submit a stateless version of the protocol (stateless-BAM) [ACGMY25] augments BAM with the eVRF [BHLS25] specified in [ACGMY25].

Secondary Crypto-Systems. This planned package submission will also include specification for additional crypto-systems that are used within the principal ones. These additional crypto-systems are optimised variants of common crypto-systems in the literature of threshold protocols which warrants their inclusion within the Threshold Call. Specifically, this planned package submission will include optimised variants of (i) the Paillier crypto-system (category S2) [Pai99], (ii) the Damgård–Fujisaki commitment scheme (category S7) [DF02], (iii) the Pedersen commitment scheme (category S7) [Ped92], and (iv) a protocol for vector oblivious linear evaluation (VOLE) instantiated with gadgets (i)–(iii) (category S7).

Additional Gadgets. To provide security against active corruptions, the principal crypto-systems of this planned package submission make frequent use of further gadgets, mainly zero-knowledge proofs (of knowledge) (ZKP(oK)s). This intended submission will therefore also specify (non-)interactive proof protocols for several languages linked to ECC relations, validity of RSA moduli, validity of parameter tuples, messages within ciphertexts or commitments, etc.

2. Specification

Organization. The planned specification will first define the relevant modular gadgets and schemes. Because the gadgets and schemes, as optimised, do not satisfy standard, general-purpose security notions, many will not be specified as full-fledged cryptosystems. Where feasible—and provided this does not lead to distorted security notions—we will present these components and gadgets as standalone cryptosystems.

1. the (single-party) Paillier homomorphic encryption scheme [Pai99] with Paillier–Blum modulus, optimised with "tough"-RSA modulus sampling ($(p-1)/2$ and $(q-1)/2$ are both products of several prime numbers noticeably smaller than $N/4$), and small-exponent randomness sampling.
2. The (single-party, multi-message) Damgård–Fujisaki commitment scheme [DF02], also optimised with tough-RSA modulus sampling.
3. The (single-party, multi-message) Pedersen commitment scheme [Ped92].
4. A two-party sender-receiver VOLE protocol built from schemes 1 and 2. To achieve active security, this crypto-system will include the specification of non-interactive ZKPoKs for the following relations:

(a) *Damgård–Fujisaki parameter validity:* For given two-message Damgård–Fujisaki parameters (N, s_1, s_2, t), the integers s_1 and s_2 are elements of the subgroup of $\mathbb{Z}_N^*$ generated by t.

(b) *Paillier modulus well-formedness:*

i. A public integer N is a Blum modulus for two private odd primes p, q congruent with 3 modulo 4.

ii. A public integer N is Paillier compatible, i.e., $\gcd(N, \varphi(N)) = 1$.

iii. A public integer N can be factored into two integers p, q that lie within a certain public range of integers.

(c) *VOLE operations:*

i. **Step 1—Receiver.** *Encrypted small discrete logarithm:* For a given Paillier ciphertext C encrypted under the receiver's public key, the encrypted plaintext $x = \mathrm{dec}(C)$ is range-checked and consistent with the discrete logarithm of a public EC point.

ii. **Step 2—Sender.** *Small coefficient Paillier affine combination:* For public Paillier ciphertexts C and D respectively encrypted under the receiver's and the sender's public key, it holds that $\mathrm{dec}(D) = a \cdot \mathrm{dec}(C) + b$ for range-checked private coefficients a, b.

The document will then specify the BAM family of crypto-systems consisting of three phases performed by the two parties, denoted as Server and Client respectively: non-interactive setup, key generation, and signing.

- **Non-Interactive Setup.** The Server samples an RSA modulus and Damgård–Fujisaki parameters and attests to their validity with non-interactive ZKPoK. The Client verifies the Server's proofs.
- **Key Generation.** A commit-open construction is used by the Server when generating its share of the ECDSA private key, but not by the Client to reduce the number of rounds in the protocol. The Client also engages in Step 1 of the VOLE protocol, and uses a non-interactive ZKPoK of discrete logarithm which will also be specified. The Server verifies the Client's proofs and completes Step 1 of the VOLE protocol.
- **Signing.** To sign, the Server samples a random share of the nonce and sends its corresponding EC point, without first committing to it, in order to save interaction rounds. The Client then engages in Step 2 of the VOLE protocol. After verifying the proof, the Server decrypts the Paillier ciphertext, reduces the value modulo the EC order, and outputs the signature if no error is detected.

While the Server and Client play different roles in the protocols described above, the computational requirements are approximately equal for both of them. However, the Server would need greater resources to be able to serve several Clients simultaneously without performance degradation.

System model. The BAM family of two-party protocols uses a *point-to-point channel* for communication. Its analysis is carried out in the *random oracle* and *generic group* models, and it relies on no additional (trusted or ideal) setup assumptions. As potential future work, we aim to show that this protocol realizes an ideal threshold-signature functionality as in [CGGMP20]. This is deferred because, to the best of our knowledge, no threshold-signature functionality currently incorporates the generic group model.

All of the BAM protocols provide security with abort against active corruption of either of the two parties.

Security. In a game-based model, security will be proven against, in turn, a corrupted Client and a corrupted Server. The security theorems assume: (i) the doubly-enhanced unforgeability of the ECDSA (which will be defined and proven), (ii) the hardness of small-exponent decisional composite residuosity, and (iii) the hardness of strong-RSA moduli.

3. Open-Source Implementation

The core code will be written in `C` and `C++17` and will be organised following the structure of the submission. There currently isn't a public repository with an implementation of the BAM protocol.

In addition to testing correctness in the all-honest scenario, the test suite will also test the behaviour of the code in case of a malicious party or an unreliable network that delays, modifies or drops messages.

4. Experimental Performance Evaluation

The current code package's performance is reported in Table 1. The 112-bit and 128-bit security levels differ in several parameters such as the bit-length of RSA moduli, the number of repetitions of certain ZKPoKs, and various slackness parameters.

Protocol	112-bit security (ms)	128-bit security (ms)
Setup	680	1 047
KeyGen	92	109
Sign	23	48

Table 1: Computation time per party of the core computation for the BAM protocol over the `secp256k1` elliptic curve, not including computation required for the networking model. Measurements obtained on Intel® Core™ i7-1365U CPU.

Platform. The baseline platform is expected to provide sufficient resources for realistic benchmarking, and we do not anticipate particular challenges.

5. Licensing, Patent Claims, and Funding

The *core code* will be open-sourced under the GPL-3.0 licence [Fre07].

The team is not aware of any patents with claims covering the content of the planned submission.

References

[ABCGJM24] Michael Adjedj, Constantin Blokh, Geoffroy Couteau, Arik Galansky, Antoine Joux, and Nikolaos Makriyannis. *Two-Round 2PC ECDSA at the Cost of 1 OLE*. Cryptology ePrint Archive, Report 2024/1950. 2024. URL: https://eprint.iacr.org/2024/1950.

[ACGMY25] Michael Adjedj, Geoffroy Couteau, Arik Galansky, Nikolaos Makriyannis, and Oren Yomtov. *Stateless 2PC Signatures for Internet-Scale Authentication and Authorization*. Cryptology ePrint Archive, Paper 2025/1475. To appear at AsiaCCS 2026. 2025. URL: https://eprint.iacr.org/2025/1475.

[BHLS25] Dan Boneh, Iftach Haitner, Yehuda Lindell, and Gil Segev. "Exponent-VRFs and Their Applications". In: *EUROCRYPT 2025, Part VII*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15607. LNCS. Springer, Cham, May 2025, pp. 195–224. DOI: 10.1007/978-3-031-91098-2_8. Also at ia.cr/2024/397.

[CGGMP20] Ran Canetti, Rosario Gennaro, Steven Goldfeder, Nikolaos Makriyannis, and Udi Peled. "UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts". In: *ACM CCS 2020*. Ed. by Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna. ACM Press, November 2020, pp. 1769–1787. DOI: 10.1145/3372297.3423367. Also at ia.cr/2021/060.

[DF02] Ivan Damgård and Eiichiro Fujisaki. "A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order". In: *ASIACRYPT 2002*. Ed. by Yuliang Zheng. Vol. 2501. LNCS. Springer, Berlin, Heidelberg, December 2002, pp. 125–142. DOI: 10.1007/3-540-36178-2_8. Also at ia.cr/2001/064.

[Fre07] Free Software Foundation. *The GNU General Public License version 3.0*. https://www.gnu.org/licenses/gpl-3.0.en.html. 2007.

[Pai99] Pascal Paillier. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *EUROCRYPT'99*. Ed. by Jacques Stern. Vol. 1592. LNCS. Springer, Berlin, Heidelberg, May 1999, pp. 223–238. DOI: 10.1007/3-540-48910-X_16.

[Ped92] Torben P. Pedersen. "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing". In: *CRYPTO'91*. Ed. by Joan Feigenbaum. Vol. 576. LNCS. Springer, Berlin, Heidelberg, August 1992, pp. 129–140. DOI: 10.1007/3-540-46766-1_9.

[NIST-IR8214C] Luís T. A. N. Brandão and René Peralta. *NIST First Call for Multi-Party Threshold Schemes*. (National Institute of Standards and Technology) NIST Internal Report (NISTIR) 8214C. 2026. DOI: 10.6028/NIST.IR.8214C.