journal of Groups, Complexity, Cryptology
Volume 17, Issue 2, 2025, pp. 1:1–1:3
https://gcc.episciences.org/

Submitted Jun. 13, 2025
Published Dec. 2, 2025

KAHROBAEI–KOUPPARIS DSS: UNIVERSAL FORGERY

ALEXANDER USHAKOV

Department of Mathematical Sciences, Stevens Institute of Technology, Hoboken NJ 07030
e-mail address: aushakov@stevens.edu

Abstract. Regardless of the choice of parameters, knowledge of a single signed message, i.e., a pair message/signature, produced by Kahrobaei-Koupparis digital signature scheme, proposed in [D. Kahrobaei and C. Koupparis, 2012], is sufficient to forge a valid signature for any other message.

1. Introduction

Digital signature schemes (DSS) are fundamental primitives in modern cryptography, ensuring message authenticity and integrity. Since their introduction, numerous group-based constructions have been proposed as alternatives to classical number-theoretic schemes, motivated by potential resistance to quantum attacks, see [4, 5, 1, 2]. In [3], Kahrobaei and Koupparis introduced a group-based DSS relying on a combination of group exponentiation and collision-resistant hashing.

In this work, we demonstrate a universal forgery attack on the Kahrobaei–Koupparis DSS: knowledge of a single valid message-signature pair allows an adversary to efficiently construct valid signatures for *any* message, regardless of the underlying group or chosen parameters. This result highlights a fundamental vulnerability in the scheme and emphasizes the importance of rigorous security analysis for group-based cryptographic constructions.

2. The Kahrobaei–Koupparis DSS scheme

Let G be a group. Fix two functions:

- $f : G \to \{0,1\}^*$, an encoding function that maps group elements to binary strings;
- $H : \{0,1\}^* \to G$, a collision-resistant hash function mapping binary strings to elements of G.

The Kahrobaei–Koupparis DSS scheme digital signature scheme consists of the following steps.

- (Key-generation) The signer first chooses
  - an element $g \in G$, whose centralizer $C(g)$ is the cyclic subgroup $\langle g \rangle$,
  - $s \in G$,

Key words and phrases: Group-based cryptography, digital signature.
2020 *Mathematics Subject Classification.* 94A62.

DOI:10.46298/jgcc.2025.17.2.16995

  - $n \in N$, where n is chosen to be highly composite.

  The private key is a pair (s, n). The public key is the element $x = g^{ns} \in G$.
- (Signing) To sign a message m, the signer chooses a random element $t \in G$ and a random factorization $n_i n_j$ of n, and computes the following (with $\|$ denoting concatenation):
  - $y = g^{n_i t}$,
  - $h = H(m \| f(y))$,
  - $\alpha = t^{-1} shy$.

  Then $sign(m) = (y, \alpha, n_j)$.
- (Verification) A given signature (y, α, n_j) for m is verified by
  - computing $h' = H(m \| f(y))$
  - verifying the identity $y^{n_j \alpha} = x^{h' y}$.

Proposition 2.1. *The scheme is correct.*

Proof. Indeed a signature constructed according to the protocol yields $h' = h$ during verification, which then results in equal elements
- $y^{n_j \alpha} = (g^{n_i t})^{n_j \alpha} = (g^{nt})^{\alpha} = g^{ntt^{-1} shy} = g^{nshy}$,
- $x^{hy} = (g^{ns})^{hy} = g^{nshy}$.

3. Forging signatures

Let (y, α, n_j) be a signature for m. Then we can compute $h = H(m \| f(y))$ and, hence,

$$\Delta = \alpha y^{-1} h^{-1},$$

which is obviously the same as $t^{-1} s$. Then for a message m' we can
- keep the same value y,
- compute $h' = H(m' \| f(y))$,
- compute $\alpha' = \Delta h' y$.

Form the tuple (y, α', n_j).

Proposition 3.1. (y, α', n_j) *passes the verification step of the scheme as a signature for* m'*.*

Proof. Indeed, during verification the value $h' = H(m' \| f(y))$ is computed. Then we can directly check that
- $y^{n_j \alpha'} = (g^{n_i t})^{n_j \alpha'} = (g^{nt})^{\alpha'} = g^{nt\Delta h' y} = g^{ntt^{-1} sh' y} = g^{nsh' y}$,
- $x^{h' y} = (g^{ns})^{h' y} = g^{nsh' y}$.

References

[1] M. I. González Vasco and R. Steinwandt. *Group Theoretic Cryptography.* CRC Press / Chapman & Hall, 2015.

[2] D. Kahrobaei, R. Flores, M. Noce, M. Habeeb, and C. Battarbee. *Applications of Group Theory in Cryptography—Post-Quantum Group-Based Cryptography*, volume 278 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2024.

[3] D. Kahrobaei and C. Koupparis. Non-commutative digital signatures using non-commutative groups. *Groups, Complexity, Cryptology*, 4, 2012.

[4] A. G. Miasnikov, V. Shpilrain, and A. Ushakov. *Group-based Cryptography.* Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser Basel, 2008.

[5] A. G. Miasnikov, V. Shpilrain, and A. Ushakov. *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*. Mathematical Surveys and Monographs. AMS, 2011.