Research Article

Vitaly Roman'kov, Alexander Ushakov*, and Vladimir Shpilrain

Algebraic and quantum attacks on two digital signature schemes

https://doi.org/10.1515/jmc-2022-0023
received July 28, 2022; accepted January 03, 2023

Abstract: In this article, we analyze two digital signature schemes, proposed in Moldovyan et al., that use finite noncommutative associative algebras as underlying platforms. We prove that these schemes do not possess the claimed property of being quantum safe. We also show that in many cases these schemes are, in fact, vulnerable to "classical" algebraic cryptanalysis.

Keywords: digital signature, algebraic cryptanalysis, quantum attack, hidden subgroup problem, post-quantum cryptography, associative algebra, noncommutative algebra

MSC 2020: 94A60

1 Introduction

In [1], the authors offered two digital signature schemes that they claimed to be quantum safe, i.e., resistant to attacks by quantum algorithms.

Here, we show that, in fact, there is a polynomial-time quantum algorithm (for solving the hidden subgroup problem) that allows one to forge digital signatures in either scheme. Note that a polynomial-time quantum algorithm for solving the hidden subgroup problem in any abelian (=commutative) group was offered in [2] (see also [3]).

Moreover, we establish that the proposed schemes are typically vulnerable even to attacks that do not use quantum algorithms.

Several other, similar, digital signature schemes including [4] and [5] can be attacked using the same approach.

We also note that in [6], the authors suggested a public key establishment protocol based on similar ideas. That protocol was attacked in [7] by a method altogether different from ours.

2 Preliminaries

In [1], the authors use a particular finite associative algebra as the platform for their scheme, but our attack is not platform specific, i.e., it works for any associative algebra that fits the general design of the scheme, as described below.

*** Corresponding author: Alexander Ushakov,** Department of Mathematical Sciences, Stevens Institute of Technology, Hoboken NJ 07030, New Jersey, United States, e-mail: aushakov@stevens.edu
Vitaly Roman'kov: Sobolev Institute of Mathematics of Russian Academy of Sciences (Omsk Branch), Omsk, Russia, e-mail: romankov48@mail.ru
Vladimir Shpilrain: Department of Mathematics, The City College of New York, NY 10031, New York, United States, e-mail: shpilrain@yahoo.com

Let $\mathbb{F}$ be a field. An associative $\mathbb{F}$-algebra (or an algebra over $\mathbb{F}$, or simply an algebra if $\mathbb{F}$ is clear from the context) is an associative ring, denoted here by $\langle \Sigma, +, \circ \rangle$, which is a vector space over $\mathbb{F}$, so that $(\alpha \cdot a) \circ b = \alpha \cdot (a \circ b) = a \circ (\alpha \cdot b)$ for all $a, b \in \Sigma$, $\alpha \in \mathbb{F}$. Here, Σ denotes the set of elements of the ring, "+" denotes the operation of addition in Σ, "$\circ$" denotes the operation of multiplication in Σ, and $\alpha \cdot b$ denotes the action of $\alpha \in \mathbb{F}$ on $b \in \Sigma$.

In [1], the authors propose to use as a platform the finite-dimensional algebra $\langle \Sigma, +, \circ, \rangle$ with a fixed basis $e_0, e_1, \ldots, e_{m-1}$. Algebra elements are written as coordinate vectors with respect to this fixed basis. As usual, the multiplication operation of two vectors $a = \sum_{i=0}^{m-1} \alpha_i e_i$ and $b = \sum_{i=0}^{m-1} \beta_i e_i$ is defined by the following formula:

$$a \circ b = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \alpha_i \beta_j (e_i \circ e_j),$$

where the products $e_i \circ e_j$ are defined by the basis vector multiplication table. In [1], each (i, j)-entry of this table had the form λe_k, where $\lambda \in \mathbb{F}$, $k = k(i, j)$. The number of basis vectors e_i was 4, and the following basis multiplication table was recommended:

$\circ$	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	μe_0	e_3	μe_2
e_2	e_0	e_1	e_2	e_3
e_3	e_1	μe_0	e_3	μe_2,

where μ is a fixed element of the ground field $\mathbb{F}$.

Now let $\langle \Sigma, +, \circ \rangle$ be an associative algebra. We say that

- $E \in \Sigma$ is the *two-sided global unit* if $\forall X \in \Sigma$ one has $E \circ X = X \circ E = X$;
- $L \in \Sigma$ is a *left-sided global unit* if $\forall X \in \Sigma$ one has $L \circ X = X$;
- $R \in \Sigma$ is a *right-sided global unit* if $\forall X \in \Sigma$ one has $X \circ R = X$;
- The local order of $W \in \Sigma$ is the least $n \in \mathbb{N}$ (if exists) such that W^n is a global (perhaps one-sided) unit.

The scheme proposed in [1] essentially uses only the $\circ$ operation defined on Σ, i.e., uses the (finite) multiplicative semigroup $\langle \Sigma, \circ \rangle$ as the platform.

We often use the following basic facts.

Lemma 2.1. *Suppose that $L \in \Sigma$ is a global left-sided unit and $A \circ B = L$. Then for any $X \in \Sigma$ and $i \in \mathbb{N}$*
(a) $(X \circ L)^i = X^i \circ L$;
(b) $(B \circ X \circ A)^i = B \circ X^i \circ A$.

3 The signature algorithms

The two proposed signature algorithms use the same public key generation procedure but slightly different signing/verification procedures. A public key is a triple Y, Z, T of elements of a semigroup $\langle \Sigma, \circ \rangle$, generated as follows.

- Generate elements $A, B, L \in \Sigma$ and $A', B', L' \in \Sigma$, where L, L' are global left-sided units satisfying
$$A \circ B = L \quad \text{and} \quad A' \circ B' = L'.$$
- Compute the local order w of B', i.e., the least $w \in \mathbb{N}$ satisfying $\forall X \in \Sigma (B')^w X = X$, i.e., $(B')^w = L''$, where L'' is a global left-side unit.
- Compute T from the equation $A \circ T = (B')^{w-1}$ (it is easy to see that $T = B \circ (B')^{w-1}$ satisfies the equation).
- Generate $N \in \Sigma$ of local order q (assumed to be a large prime number).
- Generate a uniformly random integer x, $0 \le x < w$, and compute $Y = B \circ N^x \circ A \circ L$.

- Compute $Z = B' \circ N \circ A'$.

To summarize:
– public information: $\langle \Sigma, \circ \rangle$, q, Y, Z, T.
– private information: A, B, A', B', L, L', L'', N, x, w.

3.1 Signature generation/verification algorithm A

A signature for a text M (encoded by an element of Σ) is a pair (v, s) generated using a (public) hash function $F_h : \Sigma \to \mathbb{Z}_q$ as follows.
- Generate a random nonnegative integer $k < q$ and compute $V = B \circ N^k \circ A'$.
- Compute $v = F_h(V)$.
- Compute $e = F_h(M)$ (it is assumed that $e \neq 0$).
- Compute $s = ke - xv \pmod q$.

A signature (v, s) for M is verified as follows.
- Compute $e = F_h(M)$.
- Compute $V' = Y^{ve^{-1}} \circ T \circ Z^{se^{-1}}$, where e^{-1} is the multiplicative inverse of e mod q.
- Compute $v' = F_h(V')$.
- The signature is accepted if $v = v'$.

It is easy to check the soundness of the described protocol. Indeed,

$$\begin{aligned} V' &= Y^{ve^{-1}} \circ T \circ Z^{se^{-1}} \\ &= (B \circ N^x \circ A \circ L)^{ve^{-1}} \circ (B \circ (B')^{w-1}) \circ (B' \circ N \circ A')^{se^{-1}} \\ &= B \circ N^{xve^{-1}} \circ B'^{w} \circ N^{(ke-xv)e^{-1}} \circ A' \\ &= B \circ N^k \circ A' = V. \end{aligned}$$

Hence, $v' = F_h(V') = F_h(V) = v$.

3.2 Signature generation/verification algorithm B

The second signature scheme is slightly different from the first one. A signature for a text M is a pair (v, s) generated using a (public) hash function F_h as follows.
- Generate a random integer $k < q$ and compute $V = B \circ N^k \circ A'$.
- Compute $v = F_h(M, V)$.
- Compute $s = k + xv \pmod q$.

A signature (v, s) for M is verified as follows.
- Compute $V' = Y^{q-v} \circ T \circ Z^s$.
- Compute $v' = F_h(M, V')$.
- The signature is accepted if $v = v'$.

3.3 Security assumption

There are several types of attack models against digital signature schemes described in [8]. Security of the above scheme A against key-only selective/universal forgery relies on computational hardness of the

following algorithmic problem. For given Y, Z, T, M, and F_h defined as earlier, compute a pair (v_k, s_k), for a parameter value $k \in \mathbb{N}$ of our choice, where

- $v_k = F_h(B \circ N^k \circ A')$,
- $s_k = k \cdot F_h(M) - x \cdot v_k \pmod q$.

4 Algebraic cryptanalysis

The proposed digital signature schemes A and B are variations of the classical ElGamal scheme (see [9], Section 11.5.2), based on an algebraic platform. Recall that in schemes A and B, x is a long-term key and k is a session key. The key k can be chosen by any user of the system, including a potential attacker. If the attacker, Eve, knows the key x, then she will be able to sign any message M for any of the two schemes A and B. It is important to also note that if Eve can calculate the parameter k for some digital signature session, then she can easily calculate x, thereby making the scheme vulnerable. Indeed, we have $x = kev^{-1} - sv^{-1} \pmod q$ (scheme A) and $x = sv^{-1} - kv^{-1} \pmod q$ (scheme B).

In [1], the authors do not actually provide any cryptographic analysis, limiting themselves to a reference to the fact that the element N is not public. Neither do they explain in scheme A what happens if $e = 0$, and therefore, e^{-1} does not exist. The following argument shows that in many cases the parameter k can be calculated by algebraic methods using the Jordan form of a matrix. In the remaining cases, it can be recovered by solving simultaneous discrete logarithm problems in the multiplicative group of a finite field, which is an extension of the ground field $\mathbb{F}$.

It is easy to see that the public element $V = B \circ N^k \circ A'$ (common to both schemes A and B) is expressed as follows:

$$\begin{aligned} V &= B \circ N^k \circ A' = B \circ L'' \circ N^k \circ A' \\ &= B \circ (B')^{w-1} \circ B' \circ N^k \circ A' \\ &= (\underbrace{B \circ (B')^{w-1}}_{T}) \circ (\underbrace{B' \circ N \circ A'}_{Z})^k = T \circ Z^k. \end{aligned}$$

To compute k from V, we use the obtained expression $V = T \circ Z^k$ as follows. Write the element T in the form $T = \sum_{i=0}^{m-1} t_i e_i$ where $e_0, \dots, e_{m-1}$ is a basis of $(\Sigma, +, \circ)$, and $t_i \in \mathbb{F}$ for $i = 0, \dots, m-1$. Right multiplication by Z defines a linear transformation of the algebra $\langle \Sigma, +, \circ \rangle$ having a matrix $A(Z)$ with respect to the basis $e_0, \dots, e_{m-1}$. With a particular basis multiplication table in [1], the matrix $A(Z)$ looks as follows:

$$A(Z) = \begin{pmatrix} z_0 & z_1 & z_2 & z_3 \\ z_1\mu & z_0 & z_3\mu & z_2 \\ z_0 & z_1 & z_2 & z_3 \\ z_1\mu & z_0 & z_3\mu & z_2 \end{pmatrix},$$

where μ is a fixed element of the ground field $\mathbb{F}$.

Proposition 4.1. *If the Jordan form of the matrix $A(Z)$ contains a cell of size ≥ 2 with nontrivial diagonal elements, then the parameter k is immediately calculated from $V = B \circ N^k \circ A' = T \circ Z^k$. In other cases (i.e., if the matrix $A(Z)$ is diagonalizable), the problem of recovering k is reduced to simultaneous discrete logarithm problems in the multiplicative group of a finite field.*

Proof. Note that $B' \circ A \circ T = (B')^w = L''$. Therefore, by solving the corresponding set of linear equations of the form $T'Te_i = e_i$, $i = 0, \dots, m-1$, one can efficiently compute an element of T' such that $T'T$ is the global left unit L'''. Then $T' \circ V = L''' \circ Z^k = Z^k$.

Let $\tilde{A}(Z)$ be the Jordan form of the matrix $A(Z)$ and let $\tilde{A}(Z) = C^{-1}A(Z)C$ for some $m \times m$ matrix C. The Jordan form exists over an extension of the ground field $\mathbb{F}$ obtained by adjoining to $\mathbb{F}$ all roots of the characteristic polynomial of the matrix $A(Z)$. Note that with the parameters suggested in [1], the matrix $A(Z)$ is a 4×4 matrix, so the characteristic polynomial has degree 4 and therefore has at most four distinct

roots. Actually, with the particular matrix $A(Z)$ (see aforementioned paragraphs), the characteristic polynomial is $\lambda^2(\lambda^2 - 2(z_0 + z_2)\lambda + (z_0 + z_2)^2 - \mu(z_1 + z_3)^2)$, so it has a root $\lambda = 0$ of multiplicity 2.

Then, one can compute the Jordan form $\tilde{A}(Z^k) = C^{-1}A(Z^k)C$ of $A(Z^k)$. Suppose $\tilde{A}(Z)$ contains a cell of the following form:

$$\begin{pmatrix} \rho & 1 & \dots \\ 0 & \rho & \dots \\ \dots & \dots & \dots \end{pmatrix}.$$

Then $\tilde{A}(Z^k)$ contains the corresponding cell of the form

$$\begin{pmatrix} \rho^k & k\rho^{k-1} & \dots \\ 0 & \rho^k & \dots \\ \dots & \dots & \dots \end{pmatrix}.$$

If $\rho \neq 0$, then one immediately recovers $k = k\rho^{k-1} \cdot \rho \cdot (\rho^k)^{-1}$.

If $\rho = 0$, then a cell in $\tilde{A}(Z^k)$ with ρ on the diagonal vanishes if $k \geq v$, where v is the size of the cell. Since there are only a few values of k with $k < v$, these values can be checked directly.

If in the matrix $\tilde{A}(Z)$ all other cells with nonzero diagonal entries are one dimensional, we obtain a set of equations of the form $\rho_i^k = v_i$, where ρ_i are nonzero diagonal elements of $\tilde{A}(Z)$. That is, we obtain simultaneous discrete logarithm problems in a finite extension of the ground field $\mathbb{F}$.

Thus, either each of the schemes A and B is vulnerable to a "classical" (i.e., not quantum) algebraic attack, or it can be attacked by the well-known quantum algorithm for computing the discrete logarithm [10]. □

A similar analysis, but for different cryptographic schemes, was done in [11] (see also [12]).

5 A quantum attack

Let $\mathbb{Z}^k$ denote the free abelian group of rank k. We say that a function $f : \mathbb{Z}^k \to \{0, 1\}^n$ *hides* a subgroup H of $\mathbb{Z}^k$ if for any $\overline{x}, \overline{y} \in \mathbb{Z}^k$ the following holds:

$$f(\overline{x}) = f(\overline{y}) \;\Leftrightarrow\; \overline{x} - \overline{y} \in H.$$

The hidden subgroup problem is an algorithmic problem of finding a subgroup H (i.e., finding a generating set of H) hidden by a given function f.

Lemma 5.1. *Consider $A, B, L, A', B', L' \in \Sigma$ such that*
- *L, L' are global left-sided units,*
- *$A \circ B = L$ and $A' \circ B' = L'$,*
- *$N \in \Sigma$ of local order q.*

Then for any $s, t \in \mathbb{Z}$

$$B \circ N^s \circ A' = B \circ N^t \circ A' \;\Leftrightarrow\; s \equiv t \bmod q.$$

Proof. The right-to-left implication follows from the assumption that N has local order q. Conversely,

$$\begin{aligned} B \circ N^s \circ A' = B \circ N^t \circ A' &\Rightarrow A \circ B \circ N^s \circ A' \circ B' = A \circ B \circ N^t \circ A' \circ B' \\ &\Rightarrow L \circ N^s \circ L' = L \circ N^t \circ L' \\ &\Rightarrow N^s \circ L' = N^t \circ L' \\ &\Rightarrow N^s \circ L' \circ N = N^t \circ L' \circ N \\ &\Rightarrow N^{s+1} = N^{t+1} \\ &\Rightarrow s \equiv t \bmod q. \end{aligned}$$

□

Proposition 5.2. *Let x and q be as defined in the beginning of Section 3. Then the function $f(i, j) = Y^i \circ T \circ Z^j$ hides the subgroup of $\mathbb{Z}^2$ generated by*

$$\left(\frac{q}{\gcd(x, q)}, 0\right), (0, q), (1, -x).$$

Proof. Indeed, $f(i, j) = Y^i \circ T \circ Z^j = (B \circ N^x \circ A \circ L)^i \circ T \circ (B' \circ N \circ A')^j = B \circ N^{ix+j} \circ A'$, and therefore,

$$\begin{aligned} f(i, j) = f(i', j') &\Leftrightarrow ix + j = i'x + j' \pmod{q} \quad \text{(by Lemma (5.4))} \\ &\Leftrightarrow (i - i')x + (j - j') = 0 \pmod{q} \\ &\Leftrightarrow (i - i', j - j') \in gp\left\langle \left(\frac{q}{\gcd(x, q)}, 0\right), (0, q), (1, -x) \right\rangle, \end{aligned}$$

where the latter notation is for "group generated by listed elements." □

Corollary 5.3. *There is a polynomial-time quantum algorithm that for a given public key (Y, Z, T) finds private x and q.*

Proof. The algorithm solves, in polynomial time, the hidden subgroup problem for the function $f(i, j)$ introduced in Proposition 5.2 by using the general quantum algorithm from [2]. It then finds a particular generating set of this subgroup. Note that every nontrivial subgroup of $\mathbb{Z}^2$ is either cyclic or two-generated, and in our case, it is actually two-generated. Computing the row-style Hermite normal form (an analogue of the reduced row-echelon form for matrices over $\mathbb{Z}$) of the 2×2 matrix of generators of H should produce the matrix whose rows are $(1, -x)$ and $(0, q)$, thus revealing x and q. □

Proposition 5.4. *Knowledge of x allows the attacker to forge signatures for the scheme A.*

Proof. To forge a signature for a plaintext M perform the following:

- Compute $e = F_h(M)$.
- Since we know x, for any choice of $k \geq 1$, we can find $i, j \geq 1$ satisfying $k = ix + j \pmod{q}$. In this case, one has $f(i, j) = Y^i \circ T \circ Z^j = B \circ N^k \circ A'$. This is our V.
- Then we compute v and s as in the algorithm in Section 3.1.

Obviously, so constructed pair (v, s) will be accepted by the verifier. □

6 Conclusion

In this article, we have reported polynomial-time quantum algorithms that successfully attack two digital signature schemes offered in [1]. We have also shown that in many cases these schemes are vulnerable even to "classical" algebraic attacks.

Similar digital signature schemes including [4] and [5] can be attacked using the same approach. In particular, the signature scheme in [4] is a special case of the scheme B described in our Section 3.2.

Acknowledgments: The research of the first author was partially funded through the Institute of Mathematics of the Siberian Branch of the Russian Academy of Sciences, project FWNF-2022-0003.

Funding information: The research of the Vitaly Roman'kov was partially funded through the Institute of Mathematics of the Siberian Branch of the Russian Academy of Sciences, project FWNF-2022-0003.

Conflict of interest: Prof. Vladimir Shpilrain is a member of the Editorial Board of the Journal of Mathematical Cryptology but was not involved in the review process of this article.

References

[1] Moldovyan D, Moldovyan A, Sklavos N. Post-quantum signature schemes for efficient hardware implementation. In: Proceedings of the 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2019), IEEE; 2019. p. 1–5.
[2] Kitaev A. Quantum measurements and the Abelian stabilizer problem. Preprint. 1995. http://arxiv.org/abs/quant-ph/9511026.
[3] Vyalyi M, Kitaev A, Shen A. Classical and quantum computation. American Mathematical Society; 2002.
[4] Moldovyan A, Moldovyan N. Post-quantum signature algorithms based on the hidden discrete logarithm problem. Comput Sci J Moldova. 2018;26:301–13.
[5] Moldovyan D, Moldovyan A, Moldovyan N. Digital signature scheme with doubled verification equation. Comput Sci J Moldova. 2020;28:80–103.
[6] Moldovyan D, Moldovyan N. A new hard problem over non-commutative finite groups for cryptographic protocols. In: Computer network security. Berlin Heidelberg: Springer; 2010. p. 183–94.
[7] Kuzmin AS, Markov VT, Mikhalev AA, Mikhalev AV, Nechaev AA. Cryptographic algorithms on groups and algebras. J Math Sci. 2017;223:629–41.
[8] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attacks. SIAM J Comput. 1988;17:281–308.
[9] Menezes A, van Oorschot P, Vanstone S. Handbook of applied cryptography. Boca Raton, Florida: CRC Press, 1996.
[10] Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput. 1997;26(5):1484–509.
[11] Roman'kov V. Cryptanalysis of a combinatorial public key cryptosystem. Groups Complexity Cryptol. 2017;9(2):125–35.
[12] Roman'kov V. Essays in algebra and cryptology: algebraic cryptanalysis. Omsk: Omsk State University; 2018.