Research Article

Sigurd Eskeland*

Cryptanalysis of a privacy-preserving authentication scheme based on private set intersection

https://doi.org/10.1515/jmc-2023-0032
received September 06, 2023; accepted October 31, 2023

Abstract: Continuous and context-aware authentication mechanisms have been proposed as complementary security mechanisms to password-based authentication for computer devices that are handled directly by humans, such as smart phones. Such authentication mechanisms incur some privacy issues as user-dependent features are revealed to the authentication server, which is assumed to be untrusted. Domingo-Ferrer et al. proposed a privacy-preserving protocol for context-aware user authentication on the basis of private set intersection and Paillier homomorphic encryption. This approach enables user authentication based on establishing the number of similarities between sampled user context data and reference context data, without revealing any plaintext data to either party. The authors claim that their scheme is secure against malicious adversaries. In this article, we show that Domingo-Ferrer et al.'s scheme is insecure by means of two undetectable attacks that reveal all user information despite the encryption. The Paillier encryption primitive has a homomorphic property that we observe not only lacks relevance but, indeed, incurs a vulnerability that is exploited in the proposed cryptanalysis. This means that special care needs to be taken considering homomorphic properties of cryptographic primitives used in cryptographic protocols. Our cryptanalysis may therefore have a general interest regarding the design of cryptographic protocols.

Keywords: cryptanalysis, cryptographic protocols, homomorphic encryption, private set intersection, continuous authentication

MSC 2020: 68P27, 94A60

1 Introduction

Continuous authentication, sometimes referred to as implicit authentication, has been proposed as a complementary security measure for computer devices that are handled directly by humans, such as smart phones, in addition to common authentication methods, such as passwords, iris recognition, etc. The supposed advantage is a passive and seamless authentication mechanism that does not require user attention and user action, such as re-typing of passwords or holding the phone in front of the face for iris recognition. While conventional authentication methods are session-oriented, meaning that the device remains unlocked during the time period of the session, the time-window of access for continuous authentication methods is smaller than for session-oriented approaches. Continuous authentication is realized by continuously monitoring and collecting certain user feature data and checking whether they are consistent with reference template data collected during user enrollment. One purported benefit of continuous authentication over session-oriented approaches is that if a smart phone for a moment becomes accessible to someone else while it is unlocked, the

* **Corresponding author: Sigurd Eskeland,** Norsk Regnesentral, Postboks 114 Blindern, 0314 Oslo, Norway, e-mail: sigurd@nr.no

continuous authentication mechanism will not recognize the other person. This will cause the authentication to fail, and the phone will lock.

Categories of continuous authentication modalities include behavioral authentication and context-aware authentication. The premise of behavioral authentication is that there is a uniqueness to the way that a person moves and acts, such as walking style, typing style, or handling of devices, and recognizing such unique patterns is sufficient for identifying the person. Behavioral modalities (or modes) include gait, screen touch (known as touch dynamics), and typing (keystroke dynamics). Biometric authentication modalities such as face and iris recognition are often considered to be continuous authentication modalities as well. Since such modalities require some user attention and are not entirely passive and seamless, they cannot be considered true continuous authentication mechanisms. Regarding context-aware user authentication, user device-specific data and location data such as GPS data, Wi-Fi access points, and cellular data may constitute the basis for user authenticity.

Continual user- and device-specific monitoring and data collection can indeed, be considered invasive as they reveal certain user actions and whereabouts while the user is in contact with the device. Concerns and skepticism have been raised in this regard. To mitigate for such privacy challenges, several privacy-preserving continuous authentication schemes have been proposed using homomorphic encryption techniques [1–7]. Homomorphic encryption is a form of encryption that allows computations to be performed on encrypted data without first having to decrypt it. Using such encryption mechanism during enrollment, the user device encrypts the reference template data. The encryptions are transmitted to the authentication server that stores them. During the ongoing authentication, the device samples and encrypts feature data that is transmitted to the authentication server. The homomorphic encryption enables the authentication server to verify whether the encrypted authentication-time data are consistent with the encrypted reference template data, while disclosure of any other information is prevented.

Domingo-Ferrer et al. [1] proposed a privacy-preserving protocol for continuous (implicit) authentication based on private set intersection. Using private set intersection, a comparison is carried out showing the (dis) similarity between the encrypted reference template and the encrypted authentication-time features. No decryption takes place and no private keys are required, and thus, no plaintext data are revealed to any party. The authors claim that their scheme "remains robust in the malicious scenario," in which a participant may deviate from the protocol.

In this article, we show that Domingo-Ferrer et al.'s scheme is insecure against a misbehaving authentication server and external adversaries. The scheme uses the Paillier encryption algorithm as a cryptographic primitive. It has a homomorphic property that we observe not only lacks relevance but, indeed, incurs a vulnerability that is exploited in the proposed cryptanalysis. This means that special care needs to be taken considering homomorphic properties of cryptographic primitives used in cryptographic protocols.

We present two attacks that, respectively, reveal reference template features and authentication-time features in plaintext. We believe that our cryptanalysis has a general interest due to the fact that the Paillier cryptosystem is commonly used as primitive in cryptographic protocols.

2 Related work

A few privacy-preserving schemes have been proposed for different types of modalities of behavior-based and context-based user authentication.

Domingo-Ferrer et al.'s privacy-preserving authentication scheme [1] is using user context feature similarities as a basis for authentication. These features are encrypted and compared by means of private set intersection comparison, using the Paillier cryptosystem [8] as a primitive. This enables us to determine (dis)similarities between encrypted reference data and input data. This scheme seems to be inspired by the private set intersection comparison scheme proposed by Freedman et al. [9]. Similar to the former, set elements are represented by polynomial roots (or coefficients), which are protected using homomorphic encryption, based on the Paillier encryption system. Their scheme is secure in the honest-but-curious adversarial model, while also an extension with regard to the malicious adversary model is proposed.

Govindarajan et al. [6] proposed a privacy-preserving protocol for touch dynamics-based authentication. Their scheme uses a private comparison protocol proposed by Erkin et al. [10] and the homomorphic DGK encryption algorithm proposed by Damgård et al. [11,12]. It could be noted that the privacy-preserving comparison is bitwise, and as such, it is inefficient.

Safa et al. [3] proposed a generic framework for privacy-preserving implicit authentication using context data, such as location data, device-specific data, wifi connection, and browsing history. It is based on homomorphic encryption (the authors suggest the Paillier encryption scheme) and order-preserving encryption to compute the similarity between encrypted input and encrypted reference templates (by means of average absolute deviation).

The privacy-preserving authentication scheme proposed by Shahandashti et al. [4] assumes context features and is based on order-preserving symmetric encryption (OPSE) and additive homomorphic encryption. The cryptographic primitives are generic, but the authors suggest the OPSE scheme proposed by Boldyreva et al. [5] and the Paillier public key scheme.

A potential limitation with context-aware modes [1,3,4] is the inability to determine whether the user is present or not. For example, if the device is stolen within a specified area, then it cannot be distinguished between a legitimate and illegitimate user.

Balagani et al. [13] proposed a periodic keystroke dynamics-based privacy-preserving authentication scheme. It is similar to the Govindarajan et al.'s protocol [6] but assumes the private comparison protocol proposed by Erkin et al. [10] and the homomorphic DGK encryption algorithm proposed by Damgård et al. [11]. This scheme has the same efficiency problems as Govindarajan et al.

Wei et al. [2] proposed a privacy-preserving authentication scheme for touch dynamics using homomorphic encryption properties. It is based on similarity scores between input and reference features using cosine similarity. The authentication server performs a comparison between the encrypted reference template (provided during enrollment) and encrypted input template sampled during authentication. The authentication server decrypts the similarity scores and compares them with a predefined threshold. The scheme was shown to be insecure in the study by Eskeland et al. [14].

3 Domingo-Ferrer et al.'s privacy-preserving authentication protocol

Domingo-Ferrer et al.'s privacy-preserving authentication protocol [1] conducts privacy-preserving set intersection comparison for finding the (dis)similarity between two encrypted data sets. The enrollment reference template is denoted X, and the authentication-time features is denoted Y. The privacy-preserving scheme in question establishes the similarity or the number of matching elements $|X \cap Y|$, of which each set element is encrypted. Note that the study by Domingo-Ferrer et al. [1] and other literature in this area consider *dissimilarity* rather than similarity, which is the inverse $1/|X \cap Y|$. A potential user is considered legitimate and is thus authenticated if the dissimilarity stays below a certain threshold; otherwise, the authentication fails.

Enrollment phase. In this phase, the client device samples s secret enrollment values $X = \{a_1, \ldots, a_s\}$ that constitute the user reference template. These are encrypted and transferred to the carrier. To do so, the client does the following computations:

(1) Generate a public key (g, n) in agreement with the Paillier cryptosystem, where g is of order n modulo n^2. For simplicity, let $g = n + 1$. The corresponding private key is not established.
(2) Generate $s + 4$ random secret integers: $(R', r_0', d, r_i | 0 \le i \le s)$ in $\mathbb{Z}_n$.
(3) Given X, compute $s + 1$ secret polynomial coefficients $(p_0, p_1, \ldots, p_s)$:

$$p(x) = \prod_{i=1}^{s}(x - a_i) = \sum_{i=0}^{s} p_i x^i. \tag{1}$$

(4) Encrypt $(p_0, p_1, \ldots, p_s)$ in agreement with the Paillier cryptosystem:

$$E(p_i) = g^{p_i} r_i^n \bmod n^2.$$

(5) Given (R', r_0', X), compute the secret integers $(r_1', \ldots, r_s')$, so that

$$R' = \begin{cases} \prod_{j=0}^{s} r_j'^{a_1^j} \bmod n^2 \\ \prod_{j=0}^{s} r_j'^{a_2^j} \bmod n^2 \\ \quad \vdots \\ \prod_{j=0}^{s} r_j'^{a_s^j} \bmod n^2. \end{cases} \tag{2}$$

More on this below.

(6) Compute $R_i^d = (r_i'/r_i)^d \bmod n^2$ for $0 \le i \le s$.

(7) The client sends the elements

$$(g, n, E(p_i), R_i^d \mid 0 \le i \le s)$$

to the carrier. The client deletes all data except (d, R'), which are kept secret.

The secret integers $(r_0', r_1', \ldots, r_s')$, cf. equation (2), can be computed by means of the polynomial coefficients of $p(x)$, R', and another random secret integer R. Equation (2) holds if

$$r_0' = R'R^{p_0} \bmod n^2 \quad \text{and} \quad r_i' = R^{p_i} \bmod n^2, \quad 1 \le i \le s, \tag{3}$$

where R is a positive integer. The correctness of equation (2) is shown by:

$$R' = \prod_{j=0}^{s} r_j'^{a_i^j} = (R'R^{p_0})(R^{p_1})^{a_i}(R^{p_2})^{a_i^2}\cdots(R^{p_s})^{a_i^s} = R'R^{p(a_i)}, \quad 1 \le i \le s$$

since $R^{p(a_i)} = R^0 = 1$.

Authentication phase. In this phase, the carrier computes the cardinality of the intersection of the enrollment samples and samples t authentication-time features $Y = \{b_1, \ldots, b_t\}$.

(1) The carrier selects a random secret integer θ, computes $s + 1$ exponentiations $E_i' = E(p_i)^\theta \bmod n^2$, and sends $(g, n, E_i', R_i^d \mid 0 \le i \le s)$ to the device of the client to be authenticated.

(2) The client generates t random secret integers $t_i \in \mathbb{Z}_n$ (these are denoted $r(i)$ in [1]), and using the secret integers (d, R'), it encrypts the sampled b_i:

$$B_i = \prod_{j=0}^{s} E_j'^{b_i^j \cdot d \cdot t_i} \bmod n^2,$$

$$\Upsilon_i = \prod_{j=0}^{s} (R_j^d)^{b_i^j \cdot t_i} \bmod n^2,$$

$$D_i = R'^{d \cdot t_i} \bmod n^2, \quad 1 \le i \le t.$$

The triplets $\{B_i, \Upsilon_i, D_i \mid 1 \le i \le t\}$ are sent to the carrier in a random order.

(3) The carrier checks each triplet whether

$$B_i \Upsilon_i^{n \cdot \theta} \stackrel{?}{\equiv} D_i^{n \cdot \theta} \pmod{n^2}, \quad 1 \le i \le t, \tag{4}$$

The correctness of equation (4) is shown as follows. Expanding the left-hand side (L.H.S) gives

$$\begin{aligned} B_i \Upsilon_i^{n \cdot \theta} &= \prod_{j=0}^{s} E_j'^{b_i^j \cdot d \cdot t_i} \left(\prod_{j=0}^{s} (R_j^d)^{b_i^j \cdot t_i} \right)^{n \cdot \theta} = \prod_{j=0}^{s} (g^{p_j} r_j^n)^{b_i^j \cdot \theta \cdot d \cdot t_i} \left(\frac{r_j'^d}{r_j^d} \right)^{b_i^j \cdot t_i \cdot n \cdot \theta} \\ &= \prod_{j=0}^{s} g^{p_j \cdot b_i^j \cdot \theta \cdot d \cdot t_i} r_j'^{b_i^j \cdot d \cdot t_i \cdot n \cdot \theta} = R'^{b_i^0 \cdot d \cdot t_i \cdot n \cdot \theta} \prod_{j=0}^{s} g^{p_j \cdot b_i^j \cdot \theta \cdot d \cdot t_i} R^{n \cdot p_j \cdot b_i^j \cdot d \cdot t_i \cdot \theta} \\ &= R'^{d \cdot t_i \cdot n \cdot \theta} \prod_{j=0}^{s} (gR^n)^{p_j \cdot b_i^j \cdot d \cdot t_i \cdot \theta} = R'^{d \cdot t_i \cdot n \cdot \theta} (gR^n)^{p(b_i) \cdot d \cdot t_i \cdot \theta}, \quad 1 \le i \le t, \end{aligned}$$

since $p(x) = \sum_{j=0}^{s} p_j x^j$ and $r_0' = R'R^{p0}$. The right-hand side (R.H.S.) of equation (4) is $D_i^{n\cdot\theta} = R'^{d\cdot t_i\cdot n\cdot\theta}$. Thus, if $p(b_i) = 0$ then $B_i Y_i^{n\cdot\theta} = R'^{d\cdot t_i\cdot n\cdot\theta}$ and equation (4) holds.

4 Cryptanalysis

In this section, we present two attacks that reveal all user information that is subject to the enrollment and authentication phases. A significant feature is that the proposed attacks are undetectable.

The adversary is the mainly the authentication server, but could, in principle, be an external party since no private keys are involved. In addition to breeching privacy, the latter could cause additional security breeches. The external adversary could simply use the disclosed enrollment reference template for any subsequent authentication session, enabling him or her to successfully masquerade as the victim.

4.1 Attack #1: Disclosing X

The following attack is used during the authentication phase by the carrier or an external adversary. It reveals the authentication-time features b_i for $p(b_i) = 0$. Consequently, the same enrollment features $(a_j \in X) = b_i$ are revealed, since $p(a_j) = p(b_i) = 0$, which, furthermore, expose the polynomial coefficients $(p_0, p_1, \ldots, p_s)$, cf. equation (1). The adversary is the mainly the authentication server, but could in principle be an external party since no private keys are involved.

Revealing $\delta_i = dt_i$. The attack follows the prescribed protocol, except in Step 1 of the authentication phase in which the carrier sends a slightly modified encryption gE_0' instead of E_0'. The remaining encryptions $(E_1', \ldots, E_s')$ are in agreement with the protocol. Since all encryptions are probabilistic due to the random exponent θ, the attack is undetectable.

In Step 2, the client returns (B_i, Y_i, D_i), $1 \le i \le t$, where B_i now expands as:

$$B_i = g^{d\cdot t_i} \prod_{j=0}^{s} E_j'^{b_i^j\cdot d\cdot t_i} \bmod n^2.$$

If $p(b_i) = 0$, then

$$z_i = \frac{B_i Y_i^{n\cdot\theta}}{D_i^{n\cdot\theta}} = \frac{g^{d\cdot t_i} R'^{d\cdot t_i\cdot n\cdot\theta}}{R'^{d\cdot t_i\cdot n\cdot\theta}} = g^{d\cdot t_i} = 1 + \mathrm{d}t_i n \pmod{n^2}, \quad 1 \le i \le t,$$

since $g = n + 1$. This allows us to recover the secret products

$$\delta_i = \frac{z_i - 1}{n} = \frac{(1 + \mathrm{d}t_i n) - 1}{n} = \mathrm{d}t_i, \quad 1 \le i \le t. \tag{5}$$

Note that the verification of equation (4) will not hold for $p(b_i) = 0$ due to the modification of E_0'.

A note on congruencies in $\mathbb{Z}_{n^2}$. Recall that t_i is selected in the domain $\mathbb{Z}_{n^2}$ in Step 2 of the authentication phase, while the recovered value $\delta_i = dt_i$ is in the smaller domain $\mathbb{Z}_n$. The group orders of the multiplicative domains $\mathbb{Z}_n^*$ and $\mathbb{Z}_{n^2}^*$ are, respectively, $\phi(n)$ and $n\phi(n)$, where $\phi(n)$ is the Euler totient function. Given that δ_i is in $\mathbb{Z}_n$ and not $\mathbb{Z}_{n^2}$, the modular congruencies, indeed, hold modulo n, since the corresponding reduction in group order compared to $\mathbb{Z}_{n^2}$ is thus n times.[1]

1 Note that since (d, t_i) are used as exponents, the relevant group order of the pertaining powers is multiplicative. Let x be a positive integer. In general, for an integer $a \in \mathbb{Z}_{n^2}$, where $a' = a \bmod n$, the congruence $x^a \equiv x^{a'} \pmod{n}$ holds, since the reduction of multiplicative group order of powers in modulo n^2 to modulo n is n.

Revealing $a_i \in X$. The carrier conducts a simple exhaustive search w.r.t. b_i given $(B_i, \delta_i, E'_0, \ldots, E'_s)$, where $\hat{b}$ is a search variable. If

$$B_i \stackrel{?}{\equiv} \prod_{j=0}^{s} E_j'^{\hat{b}^j \cdot \delta_i} \pmod{n}$$

holds, then $\hat{b} = (b_i \in Y) = (a_j \in X)$. Given X, the secret $(p_0, p_1, \ldots, p_s)$ are found in agreement with equation (1). The search is feasible due to the limited domain of the sampled values.

4.2 Attack #2: Disclosing Y

While the previous attack only reveals the enrollment reference template X and the pertaining polynomial coefficients $(p_0, p_1, \ldots, p_s)$, the following attack discloses any element in Y. A prerequisite is a single tuple (D_k^*, δ_k^*), where D_k^* is a genuine element $D_k = R'^{d \cdot t_k^*}$, $1 \le k \le s$, of a previous session[2] by which $\delta_k^* = dt_k^*$, cf. equation (5), is obtained by means of Attack #1.

The present attack goes like follows. The carrier generates $s + 1$ large random integers θ_j, $0 \le j \le s$, not a single θ. Instead of computing $E_i' = E(p_i)^\theta$ in Step 1 of the authentication phase, the carrier computes and sends

$$E_i' = D_k^{*\theta_i} \bmod n^2, \quad 0 \le i \le s,$$

to the client together with the genuine elements $(g, n, R_i^d \mid 0 \le i \le s)$, who then responds by sending $\{B_i, Y_i, D_i \mid 1 \le i \le t\}$ to the carrier. Thanks to that the exponents θ_j, $0 \le j \le s$, are distinct and random, the pertaining elements E_j' are indistinguishable from genuine encryptions. The attack is therefore not detectable.

Given (B_i, D_i, δ_k^*), the carrier conducts a simple exhaustive search, where $\hat{b}$ is a search variable. If

$$B_i \stackrel{?}{\equiv} D_i^{\delta_k^* \cdot \sum_{j=0}^{s} \theta_j \cdot \hat{b}^j} \pmod{n}, \quad 1 \le i \le t, \tag{6}$$

holds, then $\hat{b} = (b_i \in Y)$. The search is feasible since the sampled values are within a small domain.

The correctness of equation (6) is shown as follows. The L.H.S expands as:

$$B_i = \prod_{j=0}^{s} E_j'^{b_i^j \cdot d \cdot t_i} = \prod_{j=0}^{s} (D_k^{*\theta_j})^{b_i^j \cdot d \cdot t_i} = R'^{d^2 \cdot t_k^* \cdot t_i \cdot \sum_{j=0}^{s} \theta_j \cdot b_i^j} \pmod{n},$$

while the R.H.S of equation (6) expands to:

$$D_i^{\delta_k^* \cdot \sum_{j=0}^{s} \theta_j \cdot \hat{b}^j} = (R'^{d \cdot t_i})^{\delta_k^* \cdot \sum_{j=0}^{s} \theta_j \cdot \hat{b}^j} \pmod{n} = R'^{d \cdot t_i \cdot (d \cdot t_k^*) \cdot \sum_{j=0}^{s} \theta_j \cdot \hat{b}^j} = R'^{d^2 \cdot t_k^* \cdot t_i \cdot \sum_{j=0}^{s} \theta_j \cdot \hat{b}^j} \pmod{n}.$$

Thus, equation (6) is consistent for $\hat{b} = (b_i \in Y)$.

As pointed out in Section 4.1, computations modulo n ensure that equation (6) is congruent regarding that t_i is selected in the domain $\mathbb{Z}_{n^2}$, while the recovered value $\delta_k^* = dt_k^*$ is in the smaller domain $\mathbb{Z}_n$.

5 Comments on Domingo-Ferrer et al.'s protocol

The enrollment security of Domingo-Ferrer et al.'s scheme is based on the secrecy of the elements $(d, R, R', r'_0, \ldots, r'_s, r_0, \ldots r_s)$, of which r'_0 is determined by the secret integers (R, R', p_0), and $(r'_1, \ldots, r'_s)$ are determined by R and the polynomial coefficients $(p_0, p_1, \ldots, p_s)$. The latter are eventually defined by the reference template features X. In summary, these features are included in:

2 The asterisk * indicates that the element originates from a previous session.

– The Paillier encryptions $E(p_i) = g^{p_i} r_i^n$.
– The nominators of the powers $R_i^d = (r_i'/r_i)^d$, where $r_0' = R' R^{p_0}$, $r_j' = R^{p_j}$, $1 \le j \le s$, in agreement with equation (2).

The secret integers r_i, $0 \le i \le s$, occur in both $(E(p_i), R_i^d)$, and are cancelled out during the verification, cf. equation (4). The secrecy of d prevents attacks aiming to eliminate factors in $(E(p_i), R_i^d)$ containing r_i, for example, by means of the extended euclidean algorithm.

A security feature is that all encryptions in the authentication phase are cryptographically tied to a specific session, whose security function would be to prevent replay attacks. In Step 1, the encrypted enrollment features $E(p_i)$ are encrypted by means of a common secret exponent θ, establishing a cryptographic tie to that session. Application of the same θ is therefore necessary during verification, cf. equation (4). In Step 2, the client computes the t triplets (B_i, Y_i, D_i), $1 \le i \le t$, using the secret exponents t_i, $1 \le i \le t$. This does not only cryptographically link these elements that session, but also establishes a unique link for each triplet. If the protocol is correctly designed, this would prevent an attacker from replaying or reusing cryptographic elements from previous sessions, and to combine such triplets, to mount a successful attack.

Considering a Paillier encryption $E(m) = g^m r^n \bmod n^2$, the plaintext factor g^m is protected by the secret encryption factor r^n, of which its additive homomorphic property is realized due to that g has group order n. However, the scheme in question neither decrypts anything nor uses the homomorphic property of the Paillier cryptosystem. A key observation is thus that utilizing Paillier encryption not only lacks relevance, but more importantly incurs an insecure protocol design as already shown.

6 Suggested fix

An immediate fix would simply to avoid the Paillier encryption and conduct *all* computations modulo n. The effect is that the Paillier generator g is discarded and that $c_i = E(p_i)$ becomes $c_i = r_i^n \bmod n$. This prevents Attack #1 (disclosure of X and δ_i), which in turn prevents Attack #2. Furthermore, protecting X from disclosure to external adversaries, prevents those adversaries from successfully posing as the victim during subsequent authentication sessions.

The polynomial coefficients $(p_0, p_1, \ldots, p_s)$ are then (via r_i', cf. equations 2 and 3) only used for establishing $R_i^d = (r_i'/r_i)^d \bmod n$, which, indeed, allows us correct polynomial evaluation in the verification step, cf. equation (4):

$$B_i Y_i^{n \cdot \theta} \stackrel{?}{\equiv} D_i^{n \cdot \theta} \pmod{n}, \quad 1 \le i \le t,$$

of which the L.H.S. expands to $B_i Y_i^{n \cdot \theta} = R'^{d \cdot t_i \cdot n \cdot \theta} R^{n \cdot p(b_i) \cdot d \cdot t_i \cdot \theta} \pmod{n}$ and the R.H.S. expands to $D_i^{n \cdot \theta} = R'^{d \cdot t_i \cdot n \cdot \theta} \pmod{n}$, $1 \le i \le t$.

7 Conclusion

Continuous and context-aware authentication have been proposed as an alternative to password-based authentication. However, such authentication mechanisms have privacy issues as certain user features and context-relevant information are submitted to the authentication server. In this study, we have considered a clever privacy-preserving protocol for context-aware authentication proposed by Domingo-Ferrer et al. that enables authentication, without revealing any user context information to the authentication server. The authors claim that their scheme is secure with regard to malicious participants.

In this study, we have presented two attacks: the first enables the authentication server to obtain the enrollment reference plaintext data despite the encryption, and the authentication-time plaintext data by means of the second attack. Due to the probabilistic nature of these attacks, they are not detectable.

The attacks exploit the fact that computations in Domingo-Ferrer et al.'s scheme are conducted in $\mathbb{Z}_{n^2}$ in compliance with the Paillier encryption scheme. However, a key observation in this article is that the additive homomorphism that the Paillier encryption scheme provide is not really used by the protocol in question. Instead, by rather conducting the computations in $\mathbb{Z}_n$, the scheme would no longer be vulnerable to the proposed attacks. This means that special care must be taken when using cryptographic primitives having homomorphic properties in cryptographic protocols, since these may also incur cryptographic vulnerabilities.

Acknowledgement: This work has been accepted for presentation at CIFRIS23, the Congress of the Italian association of cryptography "De Componendis Cifris."

Funding information: Parts of this research have been supported by basic institute funding at Norsk Regnesentral, RCN Grant Number 342640, and the NORCICS project, RCN Grant Number 310105.

Conflict of interest: The authors state no conflict of interest.

References

[1] Domingo-Ferrer J, Wu Q, Blanco-Justicia A. Flexible and robust privacy-preserving implicit authentication. In: IFIP International Information Security and Privacy Conference. vol 455 of IFIP Advances in Information and Communication Technology. Springer International Publishing; 2015. p. 18–34.

[2] Wei F, Vijayakumar P, Kumar N, Zhang R, Cheng Q. Privacy-preserving implicit authentication protocol using cosine similarity for internet of things. IEEE Internet Things J. 2020;8(7):5599–606.

[3] Safa NA, Safavi-Naini R, Shahandashti SF. Privacy-preserving implicit authentication. In: IFIP International Information Security Conference. Springer; 2014. p. 471–84.

[4] Shahandashti SF, Safavi-Naini R, Safa NA. Reconciling user privacy and implicit authentication for mobile devices. Comput Security. 2015;53:215–33.

[5] Boldyreva A, Chenette N, Lee Y, O'Neill A. Order-preserving symmetric encryption. In: Proceedings of the 28th Annual International Conference on Advances in Cryptology - EUROCRYPT 2009 - Volume 5479. Berlin, Heidelberg: Springer-Verlag; 2009. p. 224–41.

[6] Govindarajan S, Gasti P, Balagani KS. Secure privacy-preserving protocols for outsourcing continuous authentication of smartphone users with touch data. In: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE; 2013. p. 1–8.

[7] Baig AF, Eskeland S. Security, privacy, and usability in continuous authentication: a survey. Sensors. 2021;21(17):5967.

[8] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: International Conference on the Theory and Aapplications of Cryptographic Techniques. Springer; 1999. p. 223–38.

[9] Freedman MJ, Nissim K, Pinkas B. Efficient private matching and set intersection. In: Cachin C, Camenisch JL, editors. Advances in Cryptology - EUROCRYPT 2004. Berlin, Heidelberg: Springer; 2004. p. 1–19.

[10] Erkin Z, Franz M, Guajardo J, Katzenbeisser S, Lagendijk I, Toft T. Privacy-preserving face recognition. In: International Symposium on Privacy Enhancing Technologies Symposium. Springer; 2009. p. 235–53.

[11] Damgåard I, Geisler M, Krøigaard M. Homomorphic encryption and secure comparison. Int J Appl Cryptography. 2008 Feb;1(1):22–31.

[12] Damgård I, Geisler M, Krígaard M. A correction to "Efficient and Secure Comparison for On-Line Auctions". IACR Cryptol ePrint Archive. 2008 Jan;2008:321.

[13] Balagani KS, Gasti P, Elliott A, Richardson A, O'Neal M. The impact of application context on privacy and performance of keystroke authentication systems. J Comput Security. 2018;26(4):543–56.

[14] Eskeland S, Baig A. Cryptanalysis of a privacy-preserving behavior-oriented authentication scheme. In: Proceedings of the 19th International Conference on Security and Cryptography - SECRYPT 2022. INSTICC. SciTePress; 2022. p. 299–304.