An Improved Parallel Interactive Feige-Fiat-Shamir Identification Scheme with almost zero soundness error and complete zero-knowledge

Dhanya R. Sarath, Megha V. Ainapurkar
Department of Computer & Information Technology
Padre Conceição College of Engineering (PCCE)
Verna, Goa, India
dhanya_reghu25@yahoo.co.in, meghav786@gmail.com

Abstract—Zero-knowledge protocols are used in some real-world applications where lighter computation and no encryption are required, for instance, securing smart card. Feige-Fiat-Shamir is one of the well-known ZKP identification schemes. However some of its security problems are the zero-knowledge not closed under parallel execution and its negligible soundness error ($2^{-k}$) that may become significant with future advanced technology. In this paper we present an improved 3-pass parallel interactive scheme with ‘almost’ zero soundness error and complete zero-knowledge. This new scheme is based on Feige-Fiat-Shamir digital signature.

Keywords—parallel, interactive, Feige-Fiat_shamir, zero soundness error, zero-knowledge.

I. INTRODUCTION

In the networks, participants need to authenticate themselves before exchanging messages. It is a great challenge to design and analyze cryptographic protocols for authentication, especially in the presence of compromised participants. For an instance, the main disadvantage of simple password protocols is that when a compromised server may impersonate its client [1]. To avoid this successful impersonation, challenge-response protocols are used, however these reveal some partial information about the client’s secret [1].

Zero-knowledge proofs [13, 15] (ZKPs) are such cryptographic protocols that do not reveal the information or secret itself during the protocol, or to any eavesdropper [2]. Table I. shows the technical definition of ZKPs [4, 9, 18]. Ali Baba’s cave problem is the best known example of ZKP [3, 13]. Prover and Verifier are the two main parties involved in ZKPs [2, 10].

<table>
<thead>
<tr>
<th>Properties</th>
<th>Assumption</th>
<th>Action done</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verifier is honest</td>
<td>Prover is honest</td>
</tr>
<tr>
<td>Completeness</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Soundness</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Zero-Knowledge</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
Randomness and timing are the other additional properties [5]. Most ZKPs are 3 pass protocols [4, 5, 18]. The ZKPs can be used in three main modes, Interactive, Parallel and Non-interactive [2, 10].

A. Soundness Error

The soundness error [6, 21] of interactive zero-knowledge has negligible probability as shown in Table II. However, since the technology is growing exponentially, in future, we may expect a scenario of ZKP security attack wherein an adversary using some high-speed parallel computation can cheat the verifier even for suggested $k=4$ and $t=5$ [4, 16, 17] such that the soundness error may become non-negligible. Hence there will be a strong desire for “zero” soundness error (as shown in Table III) i.e., successful authentication of an adversary should be made “impossible”.

<table>
<thead>
<tr>
<th>Properties</th>
<th>Successful Authentication of Adversary</th>
<th>Unsuccessful Authentication of Adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soundness</td>
<td>With probability $2^{-k}$</td>
<td>With probability $1 - 2^{-k}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Properties</th>
<th>Successful Authentication of Adversary</th>
<th>Unsuccessful Authentication of Adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soundness</td>
<td>Impossible</td>
<td>Always</td>
</tr>
</tbody>
</table>

B. Weak Zero-Knowledge

When ZKPs are executed in parallel interactive mode, zero-knowledge property may not always be satisfied [7, 8, 10, 14]. This property must be achieved without increasing the accreditation [2] and slowing down the communication.

II. ANALYSIS OF FEIGE-FIAT-SHAMIR (FFS) IDENTIFICATION SCHEME

The Feige-Fiat-Shamir [4, 12, 16] (FFS) identification scheme [19] is a variation of Fiat-Shamir [11] identification scheme. This scheme is based on the difficulty of finding the square-root modulo large composite integer whose factorization is unknown [4, 12, 16]. The normal operation of simplified FFS identification scheme [16, 20] is shown in Fig. 1. and its parallel interactive mode in Fig. 2.

![Simplified FFS identification scheme for one round](image)
An Improved Parallel Interactive Feige-Fiat-Shamir Identification Scheme with almost zero soundness error and complete zero-knowledge

![Fig. 2. FFS in parallel version](image)

A. Simulation

To prove that the soundness error and weak zero-knowledge property exist practically under parallel interactive composition, an experiment has been conducted using cheating Alice theorem [20] and cheating Bob theorem [20] using FFS identification scheme with artificially small parameters. The trusted center T selects the primes \( p = 683, q = 811 \), and publishes \( n = pq = 553913 \). Integers \( k=3 \) and \( t=5 \) are defined as security parameters.

1. Prover does the following.
   (a) Selects 3 random integers \( s_1 = 157, s_2 = 43215, s_3 = 4646 \), and 3 bits \( b_1 = 1, b_2 = 0, b_3 = 1 \).
   (b) Computes \( v_1 = -112068, v_2 = 338402, \) and \( v_3 = -429490 \).
   (c) Prover’s public key is \((-112068, 338402, 124423; -429490)\) and private key is \((157, 43215, 4646)\).

2. For soundness error
   a) Adversary gets the public key \((-112068, 338402, 124423; -429490)\) and tries to impersonate the prover.
   b) Verifier generates the challenge bit set randomly.

3. For zero-knowledge
   a) Adversary gets the public key \((-112068, 338402, 124423; -429490)\) and tries to impersonate the verifier.
   b) Adversary generates the challenge bit set randomly.

B. Security Analysis of Soundness Error

When \( k=1, t=1 \) the simulation runs according to the cheating Alice theorem. However, when \( k>1 \) and \( t>1 \), Adversary can find \( \sqrt[n]{v^k} \) only if the challenge bit set contains either
   - all 0 bits or
   - single 1 bit.

Thus we need to avoid such challenge bit set in order to eliminate the soundness error. However, Adversary can still find \( \sqrt[n]{v^k} \) if he re-computes \( x \) as in Eq. 1 and with a set of random numbers for \( y_2 \).

\[
x = r^2 v_1^{b_1} \mod n \quad \ldots \ldots \ldots 1
\]

Table IV shows that adversary could successfully impersonate the prover only if he guessed correctly the challenge to be sent by the verifier. After successful impersonation, Table V shows that adversary could find the secret using Eq. 1. It is found that the values of \( \sqrt[n]{(v^t)} \) remain the same in any iteration, even if \( r \) value is changed randomly. For an instance, when \( v_2=338402, \) at \( t=2, \) the values of \( \sqrt[n]{(v^t)} \) are \((43215, 114930, 438983, 510698)\) and at \( t=5, \) the values of \( \sqrt[n]{(v^t)} \) are \((43215, 438983, 114930, 510698)\). If the number of bits of \( n \) ranges 512-1024, it is agreed that the soundness error is negligible. However this error cannot be negligible forever. This experiment concludes with the need of elimination of soundness error without increasing the computational time.

<table>
<thead>
<tr>
<th>T</th>
<th>r (or y1)</th>
<th>Challenge bits</th>
<th>Did Adversary guess the correct challenge?</th>
<th>Successful impersonation?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>497</td>
<td>0 0 0</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

Table IV. Result of Soundness Error
### Table V. Result of Soundness Error with Secret Revealed

<table>
<thead>
<tr>
<th>T</th>
<th>y1</th>
<th>Public key</th>
<th>x</th>
<th>y2</th>
<th>√(v⁻¹)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>6</td>
<td>-112068</td>
<td>157057</td>
<td>71554</td>
<td>197230</td>
</tr>
<tr>
<td></td>
<td></td>
<td>338402</td>
<td>550299</td>
<td>4076</td>
<td>43215</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-429490</td>
<td>505989</td>
<td>187658</td>
<td>4646</td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td>-112068</td>
<td>225</td>
<td>2355</td>
<td>157</td>
</tr>
<tr>
<td></td>
<td></td>
<td>338402</td>
<td>254369</td>
<td>10190</td>
<td>43215</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-429490</td>
<td>225</td>
<td>69690</td>
<td>4646</td>
</tr>
</tbody>
</table>

### Table VI. Result of Weak Zero-Knowledge

<table>
<thead>
<tr>
<th>t</th>
<th>y1</th>
<th>Challenge</th>
<th>Public key</th>
<th>x</th>
<th>y2</th>
<th>√(v⁻¹)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>551972</td>
<td>101</td>
<td>-112068</td>
<td>281188</td>
<td>24701</td>
<td>157</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>338402</td>
<td>443556</td>
<td>22286</td>
<td>510698</td>
</tr>
</tbody>
</table>

### C. Security Analysis of Weak Zero-Knowledge

Table VI shows that adversary impersonating as the verifier could find the secret of the prover using Eq. 1 in every iteration. This is because the adversary need not guess the challenge and have choice to randomly generate the challenge to find the secret. This practically proves that zero-knowledge is not closed under parallel interactive composition. This experiment concludes with the need to achieve complete zero-knowledge.
An Improved Parallel Interactive Feige-Fiat-Shamir Identification Scheme with almost zero soundness error and complete zero-knowledge

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-12068</td>
<td>427716</td>
<td>338402</td>
</tr>
<tr>
<td></td>
<td>-12068</td>
<td>531591</td>
<td>338402</td>
</tr>
<tr>
<td></td>
<td>-12068</td>
<td>121679</td>
<td>338402</td>
</tr>
<tr>
<td></td>
<td>-12068</td>
<td>531591</td>
<td>338402</td>
</tr>
<tr>
<td></td>
<td>-12068</td>
<td>121679</td>
<td>338402</td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>407494</td>
<td>000</td>
<td>35159</td>
</tr>
<tr>
<td></td>
<td>196812</td>
<td>111</td>
<td>33921</td>
</tr>
</tbody>
</table>

III. ANALYSIS OF FEIGE–FIAT–SHAMIR DIGITAL SIGNATURE

In this non-interactive scheme, one-way hash function plays the role of verifier [4]. It is zero-knowledge under parallel composition [22]. This scheme is prone to soundness error since verification is done only for the first $k$ bits of $e$ and $e'$ as shown in the Fig. 3. Thus, the probability of successful impersonation is $1/2^k$. In order to reduce this probability, it is better to verify all the bits of $h(m||u)$ with $h(m||w)$. Then the verifier will be convinced that the prover is honest except for hash collision.
IV. OUR SCHEME (NEW_FFS)

This 3-pass scheme is based on the FFS digital scheme; however it requires the verifier to be online in order to acknowledge the witness phase. The main aim of the scheme is even if the adversary guesses the challenge; it should not be able to:

- successfully impersonate and/or
- find the secret

A. Description

We use the same notations and the same parameters of the interactive FFS scheme such as security parameters \(k\) and \(t\), common modulus \(n\), witness \(x\), random challenge bit set \(e_1,\ldots, e_k\), private key set \(s_1,\ldots, s_k\) and public key set \(v_1,\ldots, v_k\).

This scheme is in fact a pseudo-interactive since one-way hash function plays the role of verifier; however the verifier should acknowledge the receipt of witness \(x'\).

B. Completeness

Since our scheme is based on non-interactive FFS, it also has completeness property.

C. Soundness

In order to decrease the soundness error we encrypt with \(h(x)\) by the multiplication modulo \(n\) with square of all the private keys as shown in the step 3 of Fig. 4. Adversary will have to find a hash collision in \(2^{h/2}\) attempts where \(h\) is within the range of bits of \(n\) (\(< 1024\) bits). Thus the probability of soundness error (or cheating probability) is \(2^{-t}2^{h/2}\) which is almost close to zero.

D. Zero-knowledge

Since our scheme is based on non-interactive FFS, it is zero-knowledge under parallel composition.
An Improved Parallel Interactive Feige-Fiat-Shamir Identification Scheme with almost zero soundness error and complete zero-knowledge

ISSN 2277-1956/V3N3-293-300

We ran the simulations of FFS and new_FFS with the bits of \( n = 1024 \), \( t = 20 \) with varying values of \( k = 10, 20, 30, 40 \) and so on. Their computational time is taken as the average of their respective computational times in 3 runs for each value of \( k \). The growth of computation time against the varying size \( k \) for FFS and new_FFS is shown in the Fig. 5.

VI. CONCLUSION

Our scheme is more secure than FFS since even if adversary guesses the challenge, it finds more difficult to impersonate successfully; thus soundness error is more negligible than usual. Its complete zero-knowledge property makes the scheme reliable for parallel interactive authentication. Its computational time is lesser than that of FFS making it suitable for authentication with high-speed and low memory such as smart cards.

REFERENCES