Privacy-Enhanced and Fair Matchmaking System
Applications and Analysis of Protocol, Architecture, and Performance

Dwight Horne and Suku Nair
AT&T Center for Virtualization at SMU
Department of Computer Science and Engineering
Southern Methodist University, Dallas, TX, 75275
rhorne@smu.edu, nair@lyle.smu.edu

Abstract—The Prom Problem (TPP) represents a class of challenges requiring fair and privacy-enhanced matchmaking with identity linked wishes (ILW). ILW are wishes linked to specific identities and are valid only in the case that all involved parties have those same wishes. In this paper we show where TPP is positioned within a taxonomy of privacy enhanced technologies (PETs) and contribute an example embodiment of a protocol that has been demonstrated to satisfy the security properties of TPP with practical performance characteristics. Moreover, we present applications beyond dating and relationships to include voting negotiations in legislative bodies, corporate mergers and acquisitions, and difficult peace or treaty negotiations to emphasize the potential of this PET. Having previously developed a proof-of-concept implementation and evaluated feasibility of computational and communication overhead, we also describe the architecture of the production system under development for use with TPP and other applications.

Keywords—The Prom Problem; Identity Linked Wishes; Privacy Enhanced Technology; Privacy-Enhanced Matchmaking; Security Applications

I. INTRODUCTION

The Prom Problem (TPP) corresponds with a special class of challenges that require fair and privacy-enhanced matchmaking involving identity linked wishes (ILW). The critical aspect of ILW is that they are linked to specific identities and are valid only in the case that all involved parties have those same wishes. In TPP, Alice wants to attend the prom (a dance of particular significance in high school) with Bob and she would like a risk-free method of determining whether Bob shares that wish. That is, the mechanism should be risk-free in the sense that only she and Bob could learn any useful information and only in the event that they share the same ILW. Furthermore, if Bob does not share her ILW, she does not even want Bob to know that she inquired about it. A solution to TPP must satisfy the following security properties, which were derived from those of [1] for privacy-enhanced matchmaking but further augmented and expanded for applicability to TPP in [2].

- Fairness
- Impersonation Resistance with ILW
- Wish Unlinkability with ILW
- User Unlinkability with ILW
- Matching Result Privacy with ILW

Considering the challenges of matchmaking in the context of TPP affords a valuable framework for threat analysis. For example, inference attacks may occur if Bob (or Eve) were to observe Alice initiating a secret-sharing protocol with him and thereby infer her wishes and intent given that the prom is approaching. Due to the fact that wishes such as this can be easily guessed while the veracity of them would be unknown, impersonation attacks are likely in attempts to discover private wishes or to effect false disclosure. Other practical threats include that of early termination attacks attempting to achieve an unfair advantage or database compromise in cases where sensitive data are stored in a data repository. The Horne-Nair (HN) protocol has been put forth as a solution to TPP [2]. The protocol has been presented in a general manner that is cryptographic algorithm agnostic although a specific proof-of-concept implementation was used to demonstrate its correctness and to assess feasibility of performance with high degrees of confidence and fairness, even when protocol execution occurs via anonymous communication channels to thwart potential traffic analysis attacks [3].

The primary contributions of this paper include an analysis of TPP and the HN protocol through the framework of a taxonomy of privacy-enhanced technologies (PETs) previously proposed by [4], recommendation of subtle improvements to the taxonomy to more directly capture important security requirements of TPP, a walk-through of an example embodiment of the HN protocol leveraging the RSA algorithm [5], and summary of a method of quantifying the fairness of the HN protocol [3]. We also reference key performance results that demonstrated the feasibility of the approach [3] and contribute a number of practical applications of a solution to TPP beyond dating and relationships to convey the significant potential benefits of this PET. Finally, we contribute an overview of the architecture of the production system under development to solve TPP with potential for use with other applications that require fair and privacy-enhanced matchmaking with ILW.

The organization of the remainder of this paper is as follows. Section II provides an analysis identifying where TPP and the HN protocol fit in a taxonomy of PETs and gives an exemplary walk-through of one embodiment of the HN protocol. Next, Sections III and IV highlight some potential applications of the PET and address the system architecture respectively. Section V then concisely contrasts with related work and Section VI provides concluding remarks and mentions some planned future research directions.
II. BACKGROUND

A. The Prom Problem and a Taxonomy of Privacy-Enhanced Technologies

Heurix, Zimmermann, Neubauer, and Fenz proposed a universal taxonomy of PETs, which are technological methods or processes concentrating on preservation of user privacy, as an approach to conducting a comparative analysis of PETs in a systematic fashion [4]. That work also attempted to categorize and compare a number of previously proposed solutions to privacy challenges but it did not include matchmaking in general, or any specific protocols for private, privacy-enhanced, or related matchmaking problems. An analysis of TPP with ILW and the HN protocol has been put forth as a solution within the framework of the aforementioned PET taxonomy yields the paths for each of the seven dimensions in Fig. 1.

The **Aim** dimension covers general goals with regard to privacy. In TPP, the first three properties of indistinguishability, unlinkability, and confidentiality are all top priorities. Just as it sounds, indistinguishability is the property of exhibiting resistance to attempts to unambiguously distinguish one entity from another. Similarly, unlinkability is the property of exhibiting resistance to attempts to associate (or link) two or more entities. In addition to these three properties, deniability might also be a desirable goal in some applications and it may also be achieved. Next, the **Aspect** dimension describes the relevant aspects of privacy associated with the PET. For TPP, achieving multi-directional anonymity is required as is privacy of content (i.e., privacy of message content and ILW). Lastly, privacy of behavior can be partially achieved via the HN protocol itself in that, while an eavesdropper could observe communication with a secret sharing database, from the messages she could not learn anything about the inquiries – neither the general wishes nor the linked identities. With the use of anonymous communication channels, privacy of behavior can be fully realized. When considering the **Data** dimension, all three dimensions of data privacy protections must be addressed including data at rest (stored), data in transit (transmitted), and data being processed. The **Foundation** dimension of the taxonomy strives to capture the technical and conceptual foundations of the PET. The cryptography attribute is determined by the asymmetric algorithms used in the HN protocol. As with the majority of PETs classified by [4], the security model attribute of the HN protocol would be categorized as computational in most implementations and this also is linked directly to the security model of the underlying asymmetric encryption as well as one-way hashing algorithms. The **Reversibility** dimension is not applicable to TPP since the ability to reverse operations is not a desired outcome (although there are likely other matchmaking situations in which it could be desirable). Meanwhile, the **Scenario** dimension is an important differentiator in that, in contrast to models often used with a trusted third party (TTP) or with semi-honest participants, TPP assumes some level of mutual distrust between clients as well as external threats including the matchmaker and passive or active adversaries. Finally, due primarily to relevant attributes of scenario, aspect, and aim dimensions, a TTP cannot be used for the matchmaker in TPP and the matchmaker of the HN protocol is thusly untrusted. Hence, the **TTP** dimension can be considered not applicable or with a frequency of “never”. Overall, this approach provides a useful framework for comparison with other PETs. Nonetheless, through the use of this general PET taxonomy to analyze TPP and the HN protocol, the most obvious issue is the lack of ability to capture the requirement for fairness. To that end, we recommend adding a **Fairness** attribute to the **Aim** dimension. Other slight modifications should also be considered to include attributes that more directly capture matchmaking goals such as impersonation resistance and matching result privacy.

B. An Example of The Horne-Nair Protocol

The HN protocol for fair and privacy-enhanced matchmaking with ILW was designed to be cryptographic algorithm agnostic for flexibility and adaptability although the asymmetric algorithm used should satisfy certain properties such as **key privacy** as described by [6]. At a high level, the protocol involves a challenge, counter-challenge, independent computation of a verification value, and gradual release of that verification value in such a way as to provide anonymity, authentication of ILW, and privacy preservation. The protocol makes use of an untrusted matchmaker akin to the public database of the Zhang-Needham protocol [7]. The HN protocol itself is anonymous in that neither identities nor pseudo-identities are included with any of the messages or stored in the database. However, anonymous communication channels can be used to provide further defense against traffic analysis attacks and the protocol has been demonstrated to be efficient even while using a combination of a virtual private network (VPN) and Tor onion routing [3]. Here let us consider a specific implementation based on the RSA algorithm [5] as well as secure one-way hash function such as SHA3-512 [8]. Initially, Alice wants to attend the prom with Bob and she wants to determine if Bob feels the same way in a fair and privacy-enhanced manner. Alice and Bob have “large” and “small” public-private key pairs denoted \{PU_{AL}, PR_{AL}\}, \{PU_{AS}, PR_{AS}\}, \{PU_{BL}, PR_{BL}\}, and \{PU_{BS}, PR_{BS}\} where the following hold true.

\[
\text{Given primes } p, q \mid p \neq q \\
n = p \times q; \phi(n) = (p - 1)(q - 1) \\
eg{e} | gcd(\phi(n), e) = 1; 1 < e < \phi(n) \\
d = e^{-1} \mod \phi(n); ed = 1 \mod \phi(n) \\
PU_{AL} = \{e, n\}, PR_{AL} = \{d, n\}
\]
Let the components of Alice’s “large” key pair be denoted \( e_{AL}, d_{AL}, \) and \( n_L \). Similarly, the components of Bob’s “small” key pair would be represented as \( e_{BS}, d_{BS}, \) and \( n_S \). Hence, a protocol execution in which Alice and Bob choose each other as the linked identities might proceed as follows. It is assumed that they use a peer-to-peer web-of-trust, PKI, 3rd party system, or another method of obtaining public keys.

**Generate Challenge.** Alice generates random data \( R_A \), computes and submits counter-challenge \( X \) where \( w \) represents generic wish “want to attend prom together,” and sends the notification of wishes with equivalent exchange [9]. After Alice and Bob gradually release bits of \( V_{AB} \) in an alternating fashion in a process that can be described as follows where, for example, \( Rel_i(b_i) \) denotes that Alice has released the \( i \)th bit.

\[
X = (w + (R_A)^{d_{AL}} \mod n_S)^{e_{BL}} \mod n_L
\]

**Receive Challenge.** Bob anonymously queries \( M \) with a \( G_i \) (e.g., representing a group such as all male students at their school) and receives challenge \( X \). He then decrypts with \( PR_{BL} \) considers generic wishes \( w \), and chooses a user with whom he might share \( w \) (i.e., Alice). At this point, he also computes and submits counter-challenge \( Y \) to \( M \).

\[
\{w + F\} = (X)^{d_{BL}} \mod n_L
\]

**Receive Counter-Challenge and Compute Verifier.** Alice subsequently queries \( M \) with \( X \) and receives the associated counter-challenge \( Y \). At this point, Alice and Bob each have the necessary components to independently compute verifier \( V_{AB} \) (that will be equivalent if and only if the parties involved share the same identity linked wishes) as follows where \( T(x) \) represents truncation of input \( x \) and \( H(y) \) denotes applying one-way hash function to input \( y \).

\[
\begin{align*}
Alice: \quad & V_{AB} = H(H(R_A) + H((T(Y)^{d_{AL}} \mod n_S)^{e_{BS}} \mod n_S)) \\
Bob: \quad & V_{AB} = H(H((F)^{e_{BS}} \mod n_S) + H(R_B))
\end{align*}
\]

**Gradual Release.** After independently computing verification value \( V_{AB} \), if Alice and Bob chose each other they would have calculated the same result. To ensure fairness, Alice and Bob gradually release bits of \( V_{AB} \) in an alternating fashion in a process that can be described as follows where, for example, \( Rel_i(b_i) \) denotes that Alice has released the \( i \)th bit.

\[
\begin{align*}
\forall b_i \in V_{AB} \mid (0 = b_i \mod 2) & \land i \neq 0, \\
Rel_i(b_i) & : Rel_{i-1}(b_{i-1}) \\
\forall b_j \in V_{AB} \mid (1 = b_j \mod 2) & \land j \neq 0, \\
Rel_i(b_i) & : Rel_{i-1}(b_{i-1})
\end{align*}
\]

If all bits released match, each user would have a certain level of confidence in the matching result, which can be calculated as \( \lambda = 1 - \varepsilon \) where error \( \varepsilon \) is \( (\frac{1}{2})^{[n/2]} \) and \( (\frac{1}{2})^{[n/2]} \) (note the difference of the ceiling versus floor operators in the exponent). During the gradual release process, if a non-matching bit is released, then a participant may release fake decoy bits thereafter.

**C. Fairness of The Horne-Nair Protocol**

Fairness in matchmaking was originally defined as joint notification of wishes with equivalent exchange [9]. After being omitted from a number of subsequent matchmaking protocols over the years (e.g., see [1,7,10-12]), it was re-introduced and more formally defined to show satisfaction of the fairness property in addition to the other properties of privacy-enhanced matchmaking with identity linked wishes [2]. In the HN protocol, it is the gradual release process involving the independently computed verification values that affords fairness despite an adversary that might attempt impersonation/masquerading to falsify the result and prevent joint notification with equivalent exchange. The following fairness index function \( f(x) \) has been proposed to quantify the fairness of executions of the HN protocol where input \( x \) is \( N \), the number of bits released [3]. Notice the distinction between the floor ([ ]) and ceiling (| ]) operators in the inner exponents.

\[
Fairness \text{ Index } f(N) = \frac{1 - (1/2)^{[N/2]}}{1 - (1/2)^{[N/2]}}
\]

This formula was inspired by Jain’s fairness index for resource allocation and the idea that fairness can be reduced to the selection of an appropriate allocation metric and quantification of equality [13]. In this context, considering matchmaking to be a special case of resource allocation with one shared resource, each user’s confidence in the matching result was selected as the allocation metric. The user would perceive unfairness if one of the participants was able to achieve a sizeable advantage. If an even number of bits are released, then \( f(x) = 0 \) and perfect fairness is achieved. In cases with an odd number of bits released, as confidence increases beyond that of simply guessing \( (\frac{1}{2}) \), fairness monotonically approaches the perfect fairness value. This relationship between the number of bits released, each user’s confidence, and the fairness index values is depicted graphically in Fig. 2. In cases with the lowest fairness index values, confidence is also low rendering the perceived advantage much less useful. In fact, an important benefit of this approach is that it can be tuned to achieve the best performance given desired confidence and fairness for a particular situation. Adaptability such as this turns out to be advantageous as the solution is applied to different matchmaking applications with ILW.
III. APPLICATIONS BEYOND DATING/RELATIONSHIPS

While we present the problem of fair and privacy-enhanced matchmaking with ILW in the context of TPP because dating and relationships are perhaps the most universal of concepts, there are actually a number of potential applications which have been considered when designing the production system. Several of those applications are now discussed.

A. Voting Negotiations in Legislative Bodies

Consider legislative bodies around the world such as the Congress or Senate in the USA, the Parliament of the United Kingdom, gatherings of royalty in monarchies, and so on. Certain issues can often be divisive and members of disparate parties or affiliations may hesitate to ever break from the expected norms. Consider a case where a particularly important piece of legislation is about to be voted on and, although Alice’s party is expected to vote Yes, she is willing and eager to vote No if and only if Bob is also willing to vote No. However, if they do not share the same ILW, Alice does not want anyone (not even Bob) to know that she inquired about it for fear that it could damage her political career. In this scenario, many threats mirror those of TPP such as the threat of inference if Alice and Bob interact directly, threats to confidentiality if a TTP were used, and ultimately threats to her career if there were a lack of fairness.

B. Corporate Mergers and Acquisitions

The process of corporate mergers and acquisitions can involve high stakes negotiations. Consider a case in which Company A would like to acquire Company B. If A discloses this publicly, B may balk at this if B’s leadership perceives A as an equal peer while they might have been open to a merger rather than acquisition. Or consider the case where Company B was already in talks with Company C about a similar venture or it may be simply that B’s leadership interprets the action as having hostile intent. These and other circumstances could result in negative press, damage to negotiating positions, and more resulting in negative impact to the companies’ stock prices, damage to reputation or consumer perceptions, and so on. This is again a case where Alice, as CEO of Company A and wanting to acquire Company B might desire a risk-free way of determining whether Bob, as CEO of Company B, shares the same ILW regarding the potential acquisition. Here again we have many of the same security and privacy requirements due to threat scenarios analogous to those of TPP.

C. Recruiting of High Level Executives

The Baldwin-Gramlich (BG) protocol that presented risk-free trustable matchmaking and its conflicting goals of authentication and anonymity was presented in the context of the problem of hiring high-level managers [9]. Even today this continues to be a challenge and the risks are amplified as higher levels of executives are considered. Company A may have a particular candidate (e.g., Alice) in mind for its Vice President, President, or CEO position and they may not want to announce an opening. Similarly, Alice may be interested in new opportunities, yet for obvious reasons she does not want to let that be known publicly. Again we see another example as the challenges of recruiting of high level executives mirror the security properties required with TPP and ILW.

D. Affluent and Institutional Investing

Buying and selling of large quantities of investment vehicles can have significant impact on the prices of those assets, volatility of the markets, and more depending on the situation. For example, an investor selling tens of thousands or millions of shares might use an algorithm to sell smaller quantities throughout the day to avoid triggering a mass sell-off, a large drop in price, or to avoid realizing other negative consequences. We mention this application disregarding specific disclosure requirements and other regulations, not to suggest bypassing such regulations, but only because such regulations can differ significantly between countries, markets, and categories of securities. Consider a case where Alice, as a decision maker for an institutional investor or as an affluent individual investor, wishes to make a large purchase of a specific security if and only if the representative of that security will offer at a certain price, take a certain action with expected positive societal impact, or other circumstances. While the cases that might require fair and privacy-enhanced matchmaking with ILW would be rare compared to the number of transactions in markets, the implications of the minority of negotiations that would benefit from a solution to TPP with ILW and consequently risk-free matchmaking could be significant.

E. Peace and Other Treaty Negotiations

The modern era is ripe with challenging treaty negotiations such as attempts at peace between hostile countries or attempts to limit proliferation of nuclear and other weapons of mass destruction. Suppose Alice and Bob represent their respective countries or other affiliations that are involved at opposing sides of a fragile situation in which there has been hostility for quite some time. Alice and Bob both have a need to appear steadfast and resolute during negotiations for the morale of their countries and the longevity of their leadership. Bob might be willing to provide concessions in a number of ways if he knew that Alice was also willing to make comparable concessions. However, neither would want that to be publicly known. In fact, it could weaken one’s position if the opponent knew they were willing to make concessions. For example, if Bob were willing to make concessions, a hostile Alice might perceive it as weakness and an opportunity to escalate tensions for a better result at the expense of Bob and his constituents. Clearly, an efficient system and method for fair and privacy-enhanced matchmaking with ILW could offer opportunities to conduct improved negotiations in a privacy-preserving way that also mitigates risks of leaks and other compromises of confidentiality that have become prevalent. The end result of applying solutions such as the HN protocol could be positive outcomes from peace and other treaty negotiations that might otherwise almost certainly be unattainable.

IV. SYSTEM DESIGN, ANALYSIS, AND LESSONS LEARNED

A. Proof-of-Concept Implementation and Feasibility Analysis

After defining TPP and its security properties, the HN protocol was developed and a proof-of-concept implementation leveraging the RSA algorithm with 4,096 bit keys was used to validate the approach. Those efforts were initially presented along with a pseudo-code example of the
Subsequently, in addition to quantifying the fairness of the protocol, implementations were refined and instrumented with high precision performance timers to facilitate testing and feasibility analysis as reported in detail in [3]. The first phase of testing focused on computational costs. Even the most computationally intensive portions of the algorithm proved practical across a range of processors from high-end to budget models, including desktop, laptop, and mobile variants. The computation of challenge and counter-challenge values had a mean runtime of less than 200 ms on even the worst performing CPU (an Intel® Atom Z3740D, 1.13 GHz) of the systems under test. In the next phase, tests quantifying real-world impacts of communication overhead were executed with a wide range of confidence and fairness values and using no anonymity approach, VPNs, Tor onion routing, and combinations thereof. Efforts focused on the gradual release process since the main protocol itself is a small constant number of rounds. Achieving high degrees of confidence and fairness were demonstrated to be practical even using combinations of VPN and Tor onion routing to afford a certain level of anonymity. For example, the test case with 99.9939% confidence and a fairness index of $0.9998779 < f(x) < 0.9999389$ exhibited mean runtimes of $3 < t < 17$ seconds depending on the anonymity approach. In reality, this reasonable performance with high degrees of confidence, fairness, and anonymity is actually even more practical than it may seem given that operations such as this would occur in the background with the user often just seeing the matching result the next time they log into the system to check status.

Achieving high degrees of confidence and fairness were demonstrated to be practical even using combinations of VPN and Tor onion routing to afford a certain level of anonymity. For example, the test case with 99.9939% confidence and a fairness index of $0.9998779 < f(x) < 0.9999389$ exhibited mean runtimes of $3 < t < 17$ seconds depending on the anonymity approach. In reality, this reasonable performance with high degrees of confidence, fairness, and anonymity is actually even more practical than it may seem given that operations such as this would occur in the background with the user often just seeing the matching result the next time they log into the system to check status. In addition to limiting risk by characterizing performance that can be expected in real-world systems and networks and thereby answering key questions of practicability, the feasibility analysis efforts also quantified relative impacts of confidence, fairness, and anonymity to guide identification of suitable tradeoffs as the solution is applied in different problem domains. Armed with confirmation of the feasibility of this approach, attention has now turned to design and development of a full-featured production system.

### B. System and Software Architecture

An overview of the software system architecture is presented in Fig. 3. The problem at hand lends itself to a client-server software architecture. In the diagram, clients are shown as possibly connected directly to the Internet or via Local Area Networks but this is not intended to exclude other connectivity options. Recall that the matchmaker is untrusted and akin to a public database although, in the system design, there is an Application Programming Interface (API) through which the Matchmaker’s services are offered. The API should simplify client application development but also afford other advantages like the opportunity to detect and prevent certain brute force attacks that might otherwise be possible with direct database access. Clients may communicate with the Matchmaker via the public Internet or via anonymous communication channels like the Tor onion routing network [16]. The high level internals of the Client application are presented for one of the client instances. It is important to note that in the HN protocol, identities are not included with any messages or stored in the Matchmaker’s database. That is desirable to avoid damage from data breaches such as the Ashley Madison hack of 2015 [17] that has allegedly led to ruined careers, damaged relationships, other unfortunate consequences, and even renewed blackmail attempts nearly two years later1. In the present system, private information will be processed on the client-side. Two important considerations are that of identity management and key management. For many applications, external identity management systems will be best suited (e.g., all Facebook®

---

or LinkedIn® users are potential users of the privacy-enhanced matchmaking system). In many cases, users are already placing some level of trust in external identity management systems such as Facebook®, the identity management system of their employer’s intranet network, and so on. Hence, in such cases there would be no additional risk from repurposing those identity management systems. But in other cases, it may be preferable to handle identity management within the client application itself such as in a peer-to-peer fashion.

The system design takes the need for flexibility into account by using a common identity management interface to hide the details of local or external identity management systems that may be needed for different applications. Similarly, keys would be generated by the clients and key management thereafter could be external (e.g., every Facebook® user has associated encryption keys – either self-generated or assigned as decoys) or it could also be handled internally such as with a web-of-trust approach resembling the trust model popularized with PGP encryption [18]. Here again the client system design leverages a common interface to simplify support for different approaches depending on the application. The interface-oriented design approach is also apparent with the interfaces for communications and cryptographic libraries for agile adaptability to support the needs of different contexts and the evolving challenges of security that is based on the computational “hardness” of a certain problem. In summary, the system architecture is designed with a variety of applications in mind from TPP and Alice’s desire to find a date in a privacy-preserving manner to voting negotiations in legislative bodies or fragile peace treaty negotiations. The absence of identities, pseudo-identities, or identity linked wishes in any protocol messages or in the Matchmaker’s database means that a compromise of the network or the Matchmaker would not result in a compromise of privacy or the confidentiality of wishes. This frees the client to handle identity and key management separately in a manner best-suited for the application at hand.

V. RELATED WORK

Table 1 contains a comparison of the matchmaking protocols most closely related to the present efforts (adapted from [2]). The dimensions of comparison in the table include a subset of the security properties that are important for TPP and ILW. With their description of trustable matchmaking and proposal of the BG protocol, Baldwin and Gramlich have been credited with seeding the line of research that has evolved surrounding variants of secure matchmaking problems [9]. The BG protocol leveraged a query-response process, fake transactions, asymmetric cryptography, a trusted third party (TTP), and anonymous communications in attempts to balance conflicting goals of anonymity and authentication to afford matchmaking with joint notification and equivalent exchange (i.e., fairness). Unfortunately, the lack of wish secrecy and reliance on a TTP for the matchmaker inhibit utility in the context of TPP. Soon thereafter, Meadows proposed a matchmaking protocol that sought wish secrecy but relied on a high degree of trust between clients [10]. Zhang and Needham later pointed out that the BG protocol was vulnerable to substitution attacks, introduced the notion of private matchmaking, and effectively argued that it had security and privacy requirements beyond mutual authentication of suspicious parties. The Zhang-Needham (ZN) protocol used the result of a one-way hash function applied to users’ wishes as an encryption key to encrypt wishes and contact information for submission to a public database. Although the ZN protocol was a clever way to locate others with the same wishes, it is vulnerable to dictionary attacks as described by [1] and that vulnerability is further amplified by a small wish space in applications such as TPP. Building on previous matchmaking efforts, Shin and Gligor rigorously defined properties of privacy-enhanced matchmaking and presented a protocol that substituted users’ wishes in place of a password in an established password authenticated key exchange (PAKE) protocol [1]. In attempts to provide some level of anonymity, they substitute pseudo-identities for identities and also use digital signatures of execution transcripts for wish authentication. But in the context of TPP with ILW, the SG protocol is vulnerable to inference attacks, impersonation attacks resulting in false disclosure or compromise of private wishes, and other threats. Furthermore, the lack of fairness with the Meadows, ZN, and SG protocols prevents their use with TPP. The lack of support for security and privacy with ILW is yet another key challenge limiting the suitability of prior protocols in this context. A number of other matchmaking and related protocols have also been proposed (e.g., [11-12,14-15]) but they differ more significantly with respect to their goals and security properties stemming from the varied problems they attempt to solve which limits direct comparison in a format comparable to Table 1. Nonetheless, those methods are susceptible to many of the same threats as the protocols of the table in addition to having other major dissimilarities that render them not applicable with TPP and ILW.

VI. CONCLUSION AND FUTURE WORK

In summary, the Prom Problem is representative of a class of challenges requiring fair and privacy-enhanced matchmaking with identity linked wishes. ILW are wishes linked to specific identities and their validity can only be determined by anonymously and fairly confirming that all linked identities share those same wishes. Thus, TPP augments the properties of privacy-enhanced matchmaking as defined by

![Table 1: Comparison of Matchmaking Protocols](image_url)

**TABLE I. COMPARISON OF MATCHMAKING PROTOCOLS [2]**

<table>
<thead>
<tr>
<th>Matchmaking Protocol</th>
<th>Subset of Matchmaking Protocol Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meadows [10]</td>
<td>Init.</td>
</tr>
<tr>
<td>Zhang/ Needham [7]</td>
<td>No</td>
</tr>
<tr>
<td>Shin/Gligor [1]</td>
<td>No</td>
</tr>
<tr>
<td>Horne/Nair [2]</td>
<td>No</td>
</tr>
</tbody>
</table>

**TABLE I. COMPARISON OF MATCHMAKING PROTOCOLS [2]**

<table>
<thead>
<tr>
<th>Matchmaking Protocol</th>
<th>Subset of Matchmaking Protocol Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meadows [10]</td>
<td>Init.</td>
</tr>
<tr>
<td>Zhang/ Needham [7]</td>
<td>No</td>
</tr>
<tr>
<td>Shin/Gligor [1]</td>
<td>No</td>
</tr>
<tr>
<td>Horne/Nair [2]</td>
<td>No</td>
</tr>
</tbody>
</table>
[1] to support security and privacy with ILW and it also adds a requirement of fairness. In this paper, the HN protocol, which has been put forth as a solution to TPP, was illustrated via walkthrough of an example embodiment derived from the RSA algorithm. A brief discussion of threats such as impersonation, inference, and early termination attacks emphasized important considerations for the problem at hand. In further efforts to convey the nature of TPP and the HN protocol in the context of the landscape of privacy-enhanced technologies, the results of an analysis leveraging the universal taxonomy of PETs proposed by [4] was presented. That exercise also led to the identification of potential enhancements to the taxonomy to better reflect certain facets of TPP and other matchmaking challenges that could serve as important differentiators. Furthermore, the analysis resulted in the realization that a fairness attribute should be considered for the Aim dimension given the potentially broad applicability of requirements for fair protocols across a range of PETs.

The context of dating and relationships provides a useful framework within which to consider TPP, one that has far-reaching appeal across disparate populations. Such a context is useful for performing a threat analysis, analyzing challenges of the problem, evaluating potential solutions, and effectively communicating related ideas. But potential applications extend far beyond courting rituals. Indeed, this paper emphasized a number of potential applications such as voting negotiations in legislative bodies, recruiting for high-level executive positions in corporations, and even as a key enabler in critical peace or other treaty negotiations. Having previously demonstrated a proof-of-concept implementation of the HN protocol as well as having characterized and quantified performance and fairness as part of overall feasibility analysis of the solution, attention turned to development of a full-featured system to realize the potential of this technology. An overview of the architecture of the system under development was also presented.

A number of avenues for future work have been identified and a few of those planned near-term include exploration of feature enhancements such as temporal constraints, geographic constraints, and detection and prevention of certain brute force attacks on the system. We also hope to evaluate the security and performance of I2P [19], mix-based solutions such as Mix-In-Place Networks [20], and Riffle [21] relative to the anonymity approaches that have already been evaluated for use in this context. Beyond development of the production system and potential enhancements, prototype web-based and mobile interfaces for each of the most impactful applications may be employed as an effective approach to conveying the potential societal benefits of this PET.

REFERENCES


