# Distance-Bounding Based Defense Against Relay Attacks in Wireless Networks

Caimu Tang, *Member, IEEE,* and Dapeng Oliver Wu, *Senior Member, IEEE*

***Abstract*—In this paper, a non-interactive zero-knowledge proof scheme is proposed for secure identification in wireless networks, and it uses a timed oblivious transfer technique to enable a single verifier to identify multiple provers. The verifier and the prover do not need to be synchronized in this scheme. This scheme also enjoys the distance-bounding property which makes the proposed scheme invulnerable to the relay attack. We propose to use the order statistic for the detection of relay attackers. We show that it is optimal in terms of minimum variance. Finally, we shed some light on implementation issues of our proposed scheme.**

***Index Terms*—Distance-bounding, non-interactive zero-knowledge proof, discrete logarithm problem, elliptic curve cryptography, timed oblivious transfer, statistical outlier test.**

## I. Introduction

RECENT years have witnessed the urgent needs to secure networks of low power wireless devices as widespread adoption of these devices in our daily life is imminent. Countermeasure of the relay attack has been one of known hard problems for many challenge-response protocols aimed at applications over these networks. The U.S. state department e-Passport or 2002 US Border Security Act (cf. [1] and references therein) mandates that anti-skimming material has to be used to countermeasure the relay attack. On ISO/IEC 18092 compatible devices where enhanced processing capability is normally present, other solutions to relay attack involving more sophisticated processing is possible.

In this paper, we will propose a solution to countermeasure relay attack which is based non-interactive zero-knowledge proof (ZKP) and uses distance-bounding technique. In general, the approach to removing the interaction in ZKP is to use a two-party oblivious transfer (OT) with offline pre-computed OT public keys [2], [3], [4], [5]. Under this approach, the prover uses the OT protocol to send messages to the verifier in multiple rounds; in each round, the prover uses a different OT public key to "encrypt" the messages. This non-interactive ZKP can enable a single verifier to identify multiple provers as the same OT public key can be used by many provers in a single round (*note that the same OT public key should not be used in different rounds*). However, relay attacks to the non-interactive ZKP can be launched as shown in Fig. 1, where the message is directional, i.e., from **P** to **V** only. In Fig. 1, $\overline{P}$, the prover and $\overline{V}$, the verifier are both under the control of an adversary, and they are located within the communication range of the legitimate prover **P** and verifier **V**. $\overline{V}$ identifies itself as a legitimate verifier to **P**, and then $\overline{P}$ can use the replies from **P** to prove its identity correctly to the legitimate **V** without being detected.

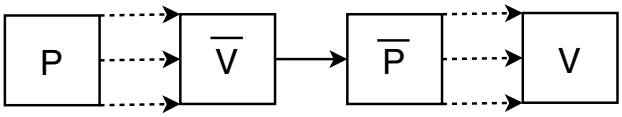


Fig. 1. Relay attack in a non-interactive ZKP protocol.

One approach to defending against the relay attack is to associate the absolute location information digitally signed along those response messages [6] sent by a prover in a challenge-response protocol. However, this approach has some limitations. For example, the global positioning system (GPS) service, which has to be employed to provide the location information, is severely limited in an indoor environment and suffers from the block-out problem under a bridge or a large solid object for outdoor use.

For the radio frequency identification (RFID) application including e-Passport, a hardware based approach has been proposed to countermeasure the relay attack; this approach uses anti-skimming material to form an inverse magnetic field to shield the tag device from clandestine scanning. A control button or personal identification number (PIN) input can be added to manually switch the device between active and inactive states so that only legitimate readers can access it at the right time. These approaches also have drawbacks, namely, inconvenience to end-users, and additional form-factor constraint.

Another approach against relay attack is to use a distance-bounding algorithm to ensure the prover is within a given distance to the verifier [7]. In this approach, the verifier and the prover each randomly generates a set of independent bits (i.e. a bitstream). The verifier sends its bitstream to the prover in a bit-by-bit fashion, after some arithmetic operations on scrambling each pair of bits at a time from the two bitstreams at the prover side (one is received from the verifier and the other is locally generated), the prover sends back the output bitstream in a bit-by-bit fashion followed by an authenticated message containing these two bitstreams signed by the prover. Then the verifier computes the round trip time (RTT) of each

Manuscript received April 20, 2006; revised August 12, 2006; accepted November 9, 2006. The editor coordinating the review of this paper and approving it for publication is X. Zhang. A short version of this paper was presented at IEEE Globecom 2006. The authors are alphabetically ordered with equal contribution.

C. Tang is with Tut Systems, Lake Oswego, OR 97035 (e-mail: ctang@tutsys.com).

D. O. Wu is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611-6130, USA (e-mail: wu@ece.ufl.edu).

Digital Object Identifier 10.1109/TWC.2007.060183.

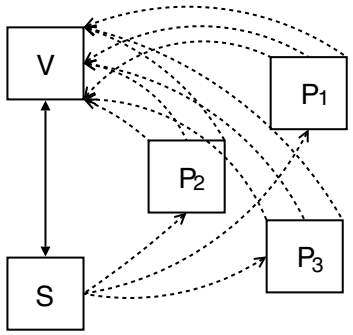


Fig. 2. Messages transmission in the proposed scheme.

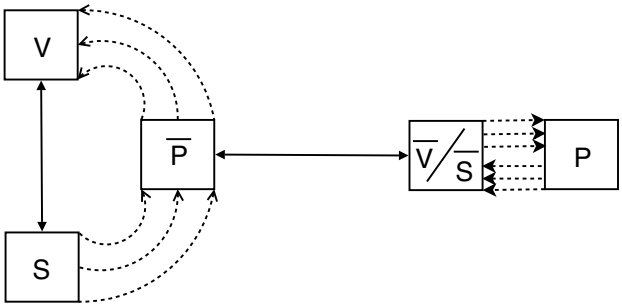


Fig. 3. Proposed scheme with a relay attacker.

bits and deviation of these RTTs. These computed RTTs will be used to determine an upper bound with a given confidence interval of the distance from the prover to the verifier. When used in a protocol to provide distance-bounding property, the verifier can reject a prover when the derived distance upper-bound is beyond a threshold even if the prover responses correctly to all challenges posed by a verifier.

Next, before we proceed, we define some notations for use throughout this paper.

**Notation:** Denote by $F$ a Galois field, and by $E$ an elliptic curve over $F$, and by $T$ an point on $E$. Further assume that the prime order $p$ of $T$ is proper for the cryptographic purpose. The additive group derived from $E$ over $F$ with respect to $T$ is denoted by $E/F$. Denote $\uplus$ as the point addition in $E/F$, and $\oplus$ as the bit-wise exclusive OR or XOR operation. $x_{(n)}$ denotes the n-th order statistic from the samples. $\lfloor x \rfloor$ denotes the largest integer less than or equal to $x$.

In this paper, we propose a scheme which allows a single verifier to identify multiple provers in an asynchronous fashion. This scheme uses elliptic curve zero-knowledge proof as the secure primitive, and uses oblivious transfer technique to enable multiple provers to be authenticated efficiently in terms of communication and computation costs. This scheme seamlessly integrates a distance-bounding algorithm so that provers' distances to the verifier can be determined, which effectively countermeasures relay attacks. Referring to Fig. 2, the server **S** broadcasts OT public keys one-by-one to a set of provers $\{\mathbf{P}_i | 1 \leq i \leq N\}$, and $\mathbf{P}_i$ then sends unidirectionally a message to **V** via the non-interactive ZKP protocol. Upon receiving the message from $\mathbf{P}_i$, the verifier **V** does not need to reply to $\mathbf{P}_i$ for aforementioned reasons such as reduction on radio interference. It can be seen that this scheme is scalable since many **P**'s can use the same OT public key during the ZKP (*note that this does not mean that the same prover will use the same OT public key pair more than once*). With this setup, the distance-bounding protocol can be seamlessly integrated into the non-interactive ZKP protocol since the transmission times of messages from provers are essentially determined by the server, rather than the provers. In other words, a delay reply is taken as having a longer time-of-flight duration. This makes the use of distance-bounding technique possible.

Prover **P** selects a random number $r$ (one time use) in a given interval, and sends **V** a point $rT$ on curve $E/F$ in a compressed form. Upon receiving an OT public key, **P** sends to **V** two numbers $(r, r + \omega)$ via OT, where $\omega$ is the private key unique to **P**. This procedure can be repeated as many times as needed to a given certainty probability of ZKP. Once the verifier **V** receives two numbers sent via OT, it records the time and obtains the duration elapsed since the OT public key is broadcasted. After a given number of executions of this procedure, the verifier can obtain a statistic to evaluate the upper-bound distance to a prover with a given confidence probability. When that distance is beyond a threshold, the prover is disqualified even if all responses provided by that prover are corrected. We propose to use the order statistic to derive the distance upper-bound. We prove that this order statistic approach is optimal, and it is easy to implement in practice as explained in Section IV.

Next we examine how this scheme defends against relay attacks to the legitimate provers. Referring to Fig. 3, $\overline{\boldsymbol{P}}$ and $\overline{\boldsymbol{V}}$ are both under the control of an adversary. Since any relay by $\overline{\boldsymbol{P}}$ and $\overline{\boldsymbol{V}}$ will significantly deviate the time duration between the time when OT public key is sent and the two messages received at the verifier, skimming can be prevented with a given confidence. Furthermore, this confidence probability can be specified by the verifier to a value which can be controlled arbitrarily close to 1.

Due to resource constraints, it is challenging to achieve synchronization for low power wireless devices [8], [9]. Existing schemes using distance-bounding technique in secure proof systems [7] require the verifier and the prover to be synchronized with high precision since a small clock drift variance may significantly reduce the distance resolution, and hence these distance-bounding based schemes are subject to high false alarm rate. The proposed scheme in this paper does not require synchronization between the verifier and the prover, and only the back-end server and the verifier need to be synchronized which is instead straightforward to achieve. This relaxation on synchronization will completely eliminate the effect of clock drift on the distance-bounding algorithm. Combined with the proposed outlier detection algorithm, our scheme is able to achieve both low false alarm rate and low false negative rate.

The rest of the paper is organized as follows. The system model and adversary model are presented in Section II. The proposed scheme is presented in Section III. Practical implementation issues are addressed in Section IV. Section V concludes this paper.

## II. System Model and Adversary Model

Due to recent algorithmic progress on solving the integer factoring problem [10] and discrete logarithm problem over finite field [11], the intractability of elliptic curve discrete logarithm problem (ECDLP) has instead been widely exploited for building many secure protocols. Let a point $Q = xT$ for $x \in [1, p-1]$, ECDLP refers to obtaining the unknown $x$ from $Q \in E/F$. When cares are exercised on the selection of the curve $E$, the point $T$ on $E$, its prime order $p$ of $T$, and the ground field $F$, the only known available algorithms to solve this well designed ECDLP will be some extensions of these square-root-type algorithms for the discrete logarithm problem over a Galois field [12] which in general have exponential complexity with regard to the key bit length. Elliptic curve cryptography (ECC) is built upon the intractability of ECDLP. One of significant advantages that ECC can bring is much shorter key length (163 bits vs. 1024 bits), hence reductions on communication cost and memory requirement. Therefore, protocols built upon ECC are more attractive for low-power devices than other asymmetric systems based on integer-factoring problem or discrete-logarithm problem over finite field.

The targeted system consists of a verifier to identify provers via verifying if a prover knows a discrete logarithm of an elliptic curve point in $E/F$ with regard to point $T \in E/F$. The server takes the role of computing the OT public keys and further distributing these public keys. The verifier **V** and the server **S** are assumed to be secure and trustworthy. It is assumed that there is a secure channel between **V** and **S**. Further assume that the verifier can capture at most one signal from multiple simultaneous transmissions from provers, and other transmissions other than the received one are considered failed. The wireless channel is assumed to have a line-of-sight (LOS) path per channel uses where an adversary may connect itself with **V** via a non-LOS link. When the server broadcasts an OT public key, all provers can receive the key within certain time intervals $x_i$; a time interval mainly consists of circuitry latency and signal propagation delay. We assume that the time intervals $x_i$ are independent and follow a uniform distribution. We also assume that the server and the verifier are synchronized. Since the server and the verifier are usually stationary, the synchronization between them can be achieved through wireline communications which is straightforward. We further assume that an adversary cannot exploit the time-of-arrival difference of multiple provers that share the same OT public key in the same round. This assumption seems reasonable noticing the fact that the provers are in a short single-hop distance from **V**, and multiple-hop relay transmissions or long haul single-hop transmissions can be eliminated by the outlier test as discussed in Section IV-A.

In this paper, all entities in the system are equipped with a wireless packet radio for information exchange. Those entities under control of an adversary may use other means of information exchange between $\overline{\boldsymbol{P}}$ and $\overline{\boldsymbol{V}}$; however, communications with **P** and **V** to/from an entity of the adversary are via the air media through the same radio transmit/receive chain on the side of **P** (radio transmit chain) and **V** (radio receive chain). Assume that there is an upper-bound of time duration on forwarding a message from **P** via $\overline{\boldsymbol{V}}$ and $\overline{\boldsymbol{P}}$ to **V**, and details are given in Section III. In addition, the adversary can eavesdrop the channel, replay all messages sent before. However, these messages exchanged are unpredictable to either an adversary or honest provers.

The computing capability of the target system of proposed scheme is asymmetric. In other words, **P** is assumed to have limited process capability with a relatively low clock-rate central process unit (CPU) while the **V** and **S** are assumed to have sufficient computing capability. Examples of a typical **P** include low-power hand-held devices. Furthermore, the radio oscillators of **V** and **S** cannot be influenced by any of **P**, good or bad. Examples of these entities include corporate server front-machines with a high clock rate CPU and timing devices which can resolve time difference in tens of nanoseconds resolution (e.g. crystal-controlled oscillator). In this paper, wireless signal time-of-flight or distance samples (in terms of packet arrival delays) is used. It is assumed that these samples can be reliably obtained. Additional details on distance resolution based on radio frequency technology are presented in Section IV.

## III. Proposed Secure Scheme Against Relay Attack

In this section, we first show the proposed N-to-1 non-interactive ZKP scheme with the use of distance-bounding technique. This scheme uses three secure primitives, namely, elliptic curve zero-knowledge proof (ECZKP) protocol, the ECDLP based elliptic curve oblivious transfer (ECOT) protocol, and distance-bounding algorithm (DBA). ECZKP is presented as Protocol 3, where ECOT is used. ECOT is presented as Protocol 2, and DBA is presented as Algorithm 1. Throughout this section, we further assume that $T'$ is a point in $E/F$ whose discrete logarithm is unknown to any entity in the system. Also note that all elliptic curve points in this paper are in compressed form as a number and represented as a binary sequence with the most significant bit position being less or equal than the specified key length in bits.

Assume that there are $n$ messages received with their corresponding durations between the time when the last bit of the ECOT public key is transmitted and the time when the first bit of the ECZKP message is received (a ECZKP message consists of a point and four numbers specified by ECZKP protocol). Further, assume that the random variables for these corresponding durations are given as $x_1, x_2, \cdots, x_n$. For the two cases without relay attacker (Case 1) and with relay attacker (Case 2), the possible minimum values of $x_i$ should not be the same, i.e. skimming is not possible when a prover is within the specified distance to the verifier (via premise surveillance for example). Since only the message in-transmit is of interest, without loss of generality, assume that the minimum value of these random variables is 0. Denote that $x_i \sim U[0, \theta]$ as a uniformly distributed random variable. Denote $\mathbf{1}[0, \theta]$ as the indicator function between 0 and $\theta$, i.e. it equals to one in $[0, \theta]$ and 0 elsewhere. To show the distance-bounding algorithm, the following lemma is needed.

*Lemma 1:* Statistic $\xi(x) = x_{(n)}$ is sufficient and complete for $\theta$; furthermore, $(n+1)\xi(x)/n$ is the minimum variance unbiased estimate of $\theta$.

*Proof:* By using the Factorization Theorem for verification of sufficient statistic and the definition of complete statistic, the first part follows. The second claim is proved via applying the Lehmann-Scheffé Theorem [13]. Refer to the Appendix A for the complete proof. ■

When **V** and **S** is synchronized, the distance-bounding algorithm is given in Algorithm 1.

*Algorithm 1:* DBA($\eta$)
$\eta$: time latency threshold.

(A) **V** obtains $n$ (a given number) response times on **P**.
- ($S_a$) (at **S**), **S** records the departure time of the first bit or symbol (for non-binary constellation) of the ECOT public key, and send the time to **V**.
- ($V_a$) (at **V**), **V** records the arrival time of the first bit or symbol of the ECZKP message, and obtain the difference of the first bit.
- ($V_b$) repeat ($S_a$) and ($V_a$) for $n$ times by **S**, and **V**, respectively, to have the vector $\boldsymbol{x}$.

(B) **V** computes $x_{(n)}$, if $x_{(n)} \geq \eta$, deny **P**.

*Remark 1:* This $x_{(n)}$ in Algorithm 1 is optimal in terms of the variance of the estimated $\theta$.

*Proof:* This remark is a direct result from Lemma 1. ■

DBA is somewhat too conservative, and it yields a low rate on false negative error (i.e. attacker succeeds) when there may be some outlier in the distribution caused by reasons including the temporary loss of line-of-sight during the proving procedure (refer to Section IV-A for details on how to address this sampling outlier issue). One possible trade-off could be to use $x_{(\lfloor n/2 \rfloor)}$ instead of $x_{(n)}$ in Step (B) of DBA as the statistic which can overcome the outlier problem in the underlying distribution. When a proper threshold and the number of repetition are selected, the false negative error rate can be controlled to a given number arbitrarily close to 0.

ECOT in this paper is 2-out-of-1 oblivious transfer protocol based on ECDLP, given a public key in the form of $(\beta_0, \beta_1)$, ECOT enables **P** to transmit to **V** two encrypted messages while **V** can decrypt only one message and **P** does not know which message **V** can decrypt. In ECOT, the public key is derived from a random bit and a random number in $[1, p-1]$. Assume that **S** is able to precompute ECOT public key as denoted by $(\beta_i, \beta_{(1-i)})_t$ before time $t$, and makes the random bit $i$ (0 or 1) and the random number $x$, which are used to generate this ECOT public key, available to **V** via a secure channel. This secure channel also ensures to **P** that the ECOT public keys come from a trustworthy part. ECZKP is a non-interactive zero-knowledge proof protocol using ECOT. When it is executed $n$ times, the certainty to **V** that **P** knows the discrete logarithm of a public key is at least $1 - \exp_2(-n)$. Using ECOT, ECZKP and DBA, the proposed N-to-1 ZKP system is given by Protocol 1.

*Protocol 1:* Assume that **S**, **V** are synchronized before the run of the protocol, and the time is slotted.

(S1) (At **S** in Slot $t$), **S** performs the following tasks in each slot:
- (S1.1) **S** selects $(i, x)_t$, where $i \in \{0, 1\}$, and $x \in [1, p-1]$, and it computes the ECOT public key $(\beta_i, \beta_{(1-i)})_t$ as shown in ECOT.
- (S1.2) **S** broadcasts $(\beta_i, \beta_{(1-i)})_t$ exactly at the end of Slot $t$.

(V2) (At **V** in Slot $t$), the following steps are executed by **V**:
- (V2.1) **V** receives $(i, x)_t$ via the secure channel.
- (V2.2) **V** receives the ECZKP message which contains five numbers, one point $rT$ in compressed form, and the four numbers given by (1) of ECOT.
- (V2.3) **V** records the arrival time of ECZKP message.
- (V2.4) **V** executes the distance-bounding algorithm on **P** as given in DBA, and disqualify **P** when both the confidence probability exceeds a threshold and the associated upper-bound distance is beyond a threshold.
- (V2.5) **V** verifies **P** as shown in Step (V1) of ECZKP.
- (V2.6) **V** repeats steps (V2.1) to (V2.5) for a predetermined number of time slots.

(P3) (At **P**), **P** executes these steps as follows:
- (P3.1) **P** executes Step (E2) of ECOT, and computes $\tilde{T}$, $\gamma$ as in Step (P1), (P2) of ECZKP.
- (P3.2) **P** receives an ECOT public key $(\beta_i, \beta_{(1-i)})_t$.
- (P3.3) **P** sends the ECZKP message based on the received ECOT public key. ■

Note that in Step (P3) of Protocol 1, upon receiving the ECOT public key, **P** needs to perform two point multiplications before the ECZKP message can be sent. However, this processing latency is taken as a constant so that the DBA algorithm can ignore this small variation if any.

*Proposition 1:* Secrecy property of Protocol 1: when the channel between **S** and **V** is secure, the overall protocol is secure.

*Proof:* There are three channels in Protocol 1, namely, the channel between **S** and **V**, the channel from **S** to **P**, and the channel from **P** to **V**. The latter two channels are insecure. The data transmitted from **P** to **V** are either uniformly distributed numbers due to encryption (causing no information leakage owing to zero knowledge proof techniques) or in the form of multiple of the base point $T$. Information contained in the latter case is protected by the intractability of ECDLP. The data transmitted from **S** to **P** are the ECOT public keys, which need not be protected. Notice the fact that these three channels are independent; therefore, the secrecy property of Protocol 1 holds. ■

We next show ECOT and ECZKP to make this paper self-contained as they are used in the proposed scheme. We then outline some properties of these protocols.

*Protocol 2:* ECOT($T', (\beta_i, \beta_{(1-i)})$)
Assume that $P$ has a pair of two numbers between 1 and $p-1$, $(n_0, n_1)$, to send to $V$.

(E1) Initialization (precomputed by $\boldsymbol{S}$): $\boldsymbol{S}$ selects a random bit $i$ (0 or 1) and a random number $x$ ($1 \leq x \leq p-1$), and computes an OT public key as $(\beta_i, \beta_{(1-i)})$ where $\beta_i = xT$ and $\beta_{(1-i)} = T' \uplus (-\beta_i)$.

(E2) $P$ verifies $\beta_0 \uplus \beta_1 = T'$, and selects two random numbers $a_0$ and $a_1$ between 1 and $p-1$, $P$ then sends the following four numbers to $V$:

$$a_0 T, a_1 T; \quad l_0 = n_0 \oplus a_0 \beta_0, l_1 = n_1 \oplus a_1 \beta_1 \qquad (1)$$

(E3) $V$ verifies (a) $\beta_i \uplus \beta_{1-i} = T'$ and (b) $n_i = l_i \oplus a_i\beta_i$ for $i = 0, 1$. ■

Note that in Protocol 2 the random bit $i$ (0 or 1) is unknown to $P$; however, the four numbers are the same as these four numbers in (2) (which may be in a different order).

$$a_iT, a_{1-i}T; \quad l_i = n_i \oplus a_i\beta_i, l_{1-i} = n_{1-i} \oplus a_{1-i}\beta_{1-i} \quad (2)$$

Assume that $y = \omega T$ is the public key. This ECZKP protocol shown next is to prove to **V** that **P** knows a secret $\omega \in [1, p-1]$ without revealing any information with regard to $\omega$ to **V** or an eveasdropper on the communication channel between **V** and **P**.

*Protocol 3:* ECZKP$(\omega, (\beta_i, \beta_{(1-i)}))$

Executes:

(P1) $P$ selects a one-time random number $1 \leq r \leq p-1$ and sends $\tilde{T} = rT$ to $V$.

(P2) $P$ computes $\gamma = r+\omega$ and sends $(r, \gamma)$ to $V$ by Protocol ECOT$(T', (\beta_i, \beta_{(1-i)}))$.

(V1) Based on the random bit $i$ selected during the initialization stage of ECOT, $V$ verifies either

$$\gamma T = \tilde{T} \uplus y \text{ if } i = 1 \quad (3)$$

or,

$$\tilde{T} = rT \text{ if } i = 0 \quad (4)$$

if (3) or (4) (with regard to $i$) holds, **V** is convinced of the case that **P** possesses $\omega$ with certainty at least a half. ■

Note that since the message is unidirectional, one single transmission containing the $\tilde{T}$ and the four numbers of ECOT is sufficient. This message is referred as the ECZKP message throughout this paper.

*Remark 2:* When there are $n$ distinct ECOT public keys precomputed and the ECZKP is repeated $n$ times with different ECOT public key, the certainty that **P** knows the discrete logarithm of $y$ is $1 - \exp_2(-n)$.

*Proof:* By following the standard argument on ZKP, each execution of ECZKP reduces the uncertainty that **P** does not know $\omega$ by at least one half. The remark follows on $n$ sequential executions of ECZKP. ■

## IV. Implementation Issues and Discussion

In this section, we shall first shed some light on how the proposed scheme can be implemented in a platform with state-of-the-art hardwares. We then shown some quantitative results on the performance of the proposed scheme. Some related issues including outlier test on time-of-flight samples are also discussed.

Distance resolution is roughly inversely proportional to the channel bandwidth allocated to the signal as shown in (5), where $\Delta d$ is the resolvable distance by a transceiver; $c$ is the speed of light in a vacuum, roughly equal to 0.3 meter per nanosecond; $f_c$ is the factor of speed of light $c$ in air with regard to $c$, and $W$ is the signal occupying bandwidth.

$$\Delta d = \frac{cf_c}{2W} \quad (5)$$

Currently, commercial radios with $TW \gg 1$ (e.g. spread-spectrum), where $T$ is the fundamental signaling interval, can resolve transmitters with apart distances in the 10 to 100 meter range [14], for example, WiFi radios use multi-channel bandwidth in the range from 22 MHz (IEEE 802.11 a/b/g/n) to 40 MHz (IEEE 802.11 g/n). Time Delay of Arrival (TDOA) technique employs the second order or higher order statistics to measure the sample correlations to derive the time delay, whence the distance can be calculated. Wireless enhanced 911 can employ TDOA distance-location technology to pinpoint wireless subscribers in carrier networks within 50 meters [15]. Approaches combining frequency delay of arrival (FDOA) and TDOA [16], [17] can achieve even better resolution. Technologies used in MIMO radios for the exploitation of multi-path scatter-rich environment are able to distinguish multi-paths in a narrow indoor environment with multiple radios a half wavelength apart to each other, e.g., 6 centimeters at 2.401 GHz minimum frequency with 22 MHz bandwidth. This type of technology can certainly be exploited for better RF distance location.

An alternative RF location technique is to use the received signal strength indicator (RSSI) to infer the sender's distance from the receiver. State-of-the-art radios can provide high precision RSSI readings (up to 32 bits) which is directly accessible to applications. When the configuration is properly set up (with only server side changes) so that it is invulnerable to various attack techniques [18], [19], [20], the deduced distances are reliable and can be used in the proposed scheme.

Henceforth, in general, with proper hardware/software support on the server side rather than handheld devices, distance-bounding technique is promising and it enjoys simplicity and more user-friendliness as compared to alternative approaches, e.g. no additional hardware limitation on handheld form-factor.

Circuitry delay of a signal after being represented in digital domain has little fluctuation even at the nanosecond level; however, analog signal processing of the waveform on the radio frequency (RF) analog front-end could introduce delay fluctuation which could enable an attacker to obtain the ECZKP message in advance the arrival time at the verifier **V**. In this case, the attacker can accelerate or slow-down to relay the ECZKP message to the verifier to perpetrate the relay attack. *It is the circuitry delay variation not the delay itself that play the key role*. However, this problem can be effectively solved via some simple modification on RF analog front-end with precise gate delay control while sacrificing some of signal-to-noise ratio (SNR) gain.

Some degree of high bit error rate is tolerable in this type of applications since repetition with automatic repeat request (ARQ) protocol can be simply employed at the verifier noticing the assumption that a verifier has no limitation on signal processing in terms of processing capability and energy. Some straightforward analysis based on Bernoulli distribution can be conducted to derive the false positive and false negative rates of the scheme. Note that as the sampling function is moving even closer to the antenna by the deployment of the emerging digital RF technology [21] using digital signal processing (DSP) operating at the gigahertz frequency level, this latency variation control on the transceiver is foreseeable not to pose any obstacle to the practical deployment of the proposed scheme.

Next for quantitative performance analysis, the overhead

incurred at the side of **S** is moderate since it involves in the generation of ECOT public keys and broadcasts these keys (or do so in advance if necessary). For **V**, it involves in only message reception, and needs to perform ECZKP verification as shown in (V1) of ECZKP, which are straightforward given the fact that both **S** and **V** are stationary. Instead, the analysis of the customer side (i.e. **P**) is focused hereafter. We use a possible customized smartcard implementation for communication costs and computation overhead, the device contains a processing unit with microcontroller unit (MCU) with clock rate at 16 MHz while a customized arithmetic logic unit (ALU) accelerator is present to facilitate point arithmetic operations (Other similar configuration includes ARM SC200 customizable smartcard implementation at 110 MHz [22]). This card is also equipped with a SmartRF CC2420 radio [23].

The curve used in this analysis is K-163 NIST curve [24] which enjoys fast algorithms on point scalar multiplication [25], [26]. It is reasonable to believe that point scalar multiplication operation on a customized smartcard chip with hardware ALU accelerator takes time in the sub-millisecond regime while the point addition operation takes time in tens of microseconds. The proposed scheme requires three point scalar multiplication operations and one point addition operation per round per prover, hence the computation time per round per prover takes around one millisecond. When other computation cost is also included, the overall computation should take time within several milliseconds (by the worst case estimate).

In each round of Protocol 1, there are one reception and one transmission per prover. Each transmitting message contains one identification number (ID), a sequence number (SEQ), ECZKP message, and the signature on the combined message of length 320 bits, where the ECZKP message contains five numbers of length 163 bits each, a SEQ which is increased by one each transmission, and also possible repeated transmissions of reply messages if erroneous bits are present and cannot be corrected. The per-bit communication cost on CC2420 radio is estimated as 0.41 $\mu$J on transmission and 0.36 $\mu$J on reception. Hence, the transmitting cost per round per prover is 0.57 mJ; Likewise, the reception cost per round per prover is 0.12 mJ. For 20 rounds with certainty at least $1 - \exp_2(-20)$ at **V**, the total communication cost is 13.8 mJ per verification. The times taken on the reception and transmission per round are around 1.2 ms and 5.6 ms, respectively. Combined with both computation time and communication latency, the overall time taken per round for executing the proposed scheme is believed within 10 ms. Note that multiple customers with different private keys can be verified at the same time, this timing performance should be sufficient for many practical applications.

### A. Outlier Issue

As noted earlier on **V** in Section III, outlier from the samples of a prover's distances can render that the n-th order statistic is not appropriate for detection of relay attackers when the outlier happens to present in the upper end of the distribution. The median order statistic may be used instead. However, the median order statistic does not preserve the nice property of being related to the upper bound of the uniform distribution. Therefore, outlier test may be used before the n-th order statistic is used.

Dixon-type discordancy test [27] uses statistics of the form $N/D$, where $N$ is a measure of the degree of separation of a sample from the rest samples, and $D$ is a measure of the degree of the spread of the samples. Dixon test statistics have been widely used in outlier test. In general, for single outlier test, most tests suffer from the masking effect if several outliers form a subgroup. However, if instead testing a group of outliers simultaneously, the swamping effect may arise due to the fact that some of non-outliers may be too close to an outlier and is mistakenly adjudged discordant along some outlier(s).

Denote by $H_0$ the null hypothesis for the case of no outliers, and $H_a$ the alternative hypothesis for the case that at least one outlier is present. For $n$ i.i.d. uniform drawn samples, the intervals between the ordered samples are then i.i.d. exponentially distributed with a common scale parameter. For outlier test on uniformly drawn samples, the following lemma was implicitly used in [28]. In this paper, we use the Dixon type F-test statistic for outlier tests for its simplicity and efficiency due to its ability of simultaneous test. Lemma 2 presents this F-test statistic. For completeness, the proof of Lemma 2 is also presented in Appendix B.

*Lemma 2:* When the samples $\{x_1, x_2, \cdots, x_n\}$ from a uniform variate are independent, under $H_0$, for an arbitrary given number $k$ ($k \in \{1, 2, \cdots, n-1\}$), then the ratio of means of $I = \{x_{(2)} - x_{(1)}, x_{(3)} - x_{(2)}, \cdots, x_{(n-k)} - x_{(n-k-1)}\}$ and $I' = \{x_{(n-k+1)} - x_{(n-k)}, \cdots, x_{(n)} - x_{(n-1)}\}$ has an F-distribution.

*Proof:* See Appendix B. ■

By Lemma 2, the following formula (cf. Equation (9) in the proof of Lemma 2)

$$\frac{E(I')}{E(I)} = \frac{n-k-1}{k} \frac{x_{(n)} - x_{(n-k)}}{x_{(n-k)} - x_{(1)}}$$

formulates the test statistic. Then the standard F-test is used to determine if a given number of $k$ outliers are present.

### B. Discussion

The number of independent timing samples is important to both the security foundation of the proposed scheme and robustness of the delay upper-bound estimate. The uncertainty probability that a **P** is an honest prover is exponentially decreasing on the number of trials. However, a large number of samples roughly linearly decreases the variance of the estimate of the delay upper bound. The solution to this sample discrepancy in a practical system is nicely addressed by the bootstrap sampling method [29], [30].

In this case, the uniform distribution assumption is immaterial to the bootstrap sampling method (i.e. this is a distribution free solution). Before the application of bootstrap, the outlier removal algorithm is still needed. Formulae based on either the n-th order statistic or the median can be used. Since **V** has sufficient computing capability, such method provides a fairly good trade-off on the communication cost reduction on the **P**.

Normality is attractive for outlier tests (e.g. Grubbs test [31]) and parameter estimation (e.g. variance on time-of-flight) for obvious reasons. One way to take advantage of many nice features of normal distribution is to derive a normally distributed random variable by central limit theorem. In this context, a fixed number of independent trials can be summed up and an approximate normal random variable is formed on consecutive sums. The uncertainty probability that a **P** is an honest prover is still individually evaluated as before. The significance probability and confidence interval can similarly be analyzed. Note that in this case, the underlying statistic distribution assumption is not important as long as the samples are obtained independently which is the case in practice.

## V. Conclusions

In this paper, a novel elliptic-curve cryptosystem based non-interactive zero-knowledge proof technique is proposed. It uses the order statistic for the optimal distance-bounding performance, and it enables the protocol invulnerable to the relay attacks. We have also shown that this scheme can be implemented efficiently with state-of-the-art wireless packet radios.

## Appendix A: Proof of Lemma 1

*Proof:* Let $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$, then the probability function of $\boldsymbol{x}$, $p(\boldsymbol{x}, \theta)$ can be expressed as follows:

$$p(\boldsymbol{x}, \theta) = \frac{1}{\theta^n}\mathbf{1}(x_{\min} \geq 0)\mathbf{1}(x_{\max} \leq \theta)$$

where, $x_{\min} = x_{(1)} = \min\{x_1, x_2, \cdots, x_n\}$ and $x_{\max} = x_{(n)} = \max\{x_1, x_2, \cdots, x_n\}$.

$p(\boldsymbol{x}, \theta)$ can be rewritten as follows:

$$p(\boldsymbol{x}, \theta) = g(\boldsymbol{x}, \theta)h(\boldsymbol{x}) \tag{6}$$

where, $h(\boldsymbol{x}) = \mathbf{1}(x_{(1)} \geq 0)$ and

$$g(\boldsymbol{x}, \theta) = \frac{1}{\theta^n}\mathbf{1}(\max\{x_1, x_2, \cdots, x_n\} \leq \theta)$$

By the Factorization Theorem and (6), $x_{(n)}$ is sufficient for $\theta$. The density function of $x_{(n)}$ is $nx^{n-1}/\theta^n$ for $0 < x < \theta$. Let

$$\int_0^\theta g(t)n\frac{t^{n-1}}{\theta^n}dt = 0, \forall\theta > 0$$

Then we have, $g(\theta) = 0, \forall\theta$. By the definition, $T(\boldsymbol{x})$ is also complete.

Since the expectation of $T(\boldsymbol{x})$ is $n\theta/(n+1)$, $(n+1)T(\boldsymbol{x})/n$ is the unbiased estimate of $\theta$. By the Lehmann-Scheffé Theorem, the second claim follows. ■

## Appendix B: Proof of Lemma 2

*Proof:* We have the sampled means of $I$ and $I'$ as follows:

$$E(I) = \frac{x_{(n-k)} - x_{(1)}}{n-k-1} \tag{7}$$

$$E(I') = \frac{x_{(n)} - x_{(n-k)}}{k} \tag{8}$$

Furthermore, $E(I)$ and $E(I')$ are independent.

Denote by $\theta$ the common scale parameter of the exponential distribution, then the random variable $Y = 2(X_{(i)} - X_{(i-1)})/\theta$ has a chi-squared distribution with degree of freedom of 2. Hence, $2E(I)/\theta$ and $2E(I')/\theta$ have chi-squared distribution with degree of freedom $2(n-k-1)$ and $2k$, respectively. Therefore, the ratio $E(I')/E(I)$ given in (9) has an F-distribution $F(2k, 2n-2k-2)$.

$$\frac{E(I')}{E(I)} = \frac{n-k-1}{k}\frac{x_{(n)} - x_{(n-k)}}{x_{(n-k)} - x_{(1)}} \tag{9}$$

■

## References


[1] A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in e-passports," in *Proc. International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2005, pp. 74–85.

[2] M. Rabin, "How to exchange secrets by oblivious transfer," Aiken's Computation Laboratory, Harvard University, Massachusetts, U.S.A., Tech. Rep. Tech. Memo TR-81, 1981.

[3] N. Koblitz, *A Course in Number Theory and Cryptography (Section: IV.5)*. Springer, 1994.

[4] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge proofs and its applications," in *Proc. 20th ACM Symposium on the Theory of Computing*, 1988, pp. 103–112.

[5] U. Feige, A. Fiat, and A. Shamir, "Zero knowledge proofs of identity," *J. of Cryptology*, vol. 1, no. 2, pp. 77–94, 1988.

[6] Y. Desmedt, "Major security problems with the 'unforgeable' (feige)-fiat-shamir proofs of identity and how to overcome them," in *Conference Record of SecuriCom, 6th Worldwide Congress on Computer and Communications Security and Protection*, 1988, pp. 15–17.

[7] S. Brands and D. Chaum, "Distance-bounding protocols," in *Lecture Notes on Computer Science (LNCS) Volume 765*. Springer-Verlag, 1993, pp. 344–359.

[8] J. van Greunen and J. Rabaey, "Lightweight time synchronization for sensor networks," in *Proc. ACM international conference on Wireless sensor networks and applications (WSNA)*, 2003, pp. 11–19.

[9] S. Ganeriwal, S. Capkun, S. Han, and M. B. Srivastava, "Secure time synchronization service for sensor networks," in *Proc. ACM Workshop on Wireless Security (WiSe)*, 2005, pp. 97–106.

[10] C. Pomerance, "Analysis and comparison of some integer factoring algorithms," in *Computational Methods in Number Theory*, J. H. W. Lenstra and R. Tijdeman, Eds. Amsterdam, The Netherlands: Mathematisch Centrum, 1982, pp. 89–139.

[11] A. M. Odlyzko, "Discrete logarithm in finite fields and their cryptographic significance," in *Proc. Eurocrypt*. Springer-Verlag, 1985, pp. 224–314.

[12] E. Teske, "Square-root algorithms for the discrete logarithm problem," in *Public Key Cryptography and Computational Number Theory*. Walter de Gruyter, 2001, pp. 283–301.

[13] G. Casella and R. L. Berger, *Statistical Inference*. Duxbury Press, 2001.

[14] G. L. Turin, "Introduction to spread-spectrum antimultipath techniques and their application to urban digital radio," *Proc. IEEE*, vol. 68, no. 3, pp. 328–353, Mar. 1980.

[15] (2005) Phase II wireless enhanced 911 location mandate. Federal Communications Commission. [Online]. Available: http://www.fcc.gov/

[16] D. C. Shin and C. L. Nikias, "Estimation of frequency-delay of arrival (FDOA) using fourth-order statistics in unknown correlated gaussian noise sources," *IEEE Trans. Signal Processing*, vol. 42, no. 10, pp. 2771–2780, Oct. 1994.

[17] A. R. Naghsh-Nilchi and V. J. Mathews, "An efficient algorithm for joint estimation of differential time delays and frequency offsets," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 1992, pp. V309–V312.

[18] A. Savvides, C. Han, and M. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proc. ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2001, pp. 166–179.

[19] D. Liu, P. Ning, and W. K. Du, "Attack-resistant location estimation in sensor networks," in *Proc. ACM/IEEE International Symposium on Information Processing in Sensor Networks (IPSN)*, 2005, pp. 99–106.

[20] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 221–232, Feb. 2006.

[21] (2005) Digital RF technology. Texas Instruments. [Online]. Available: http://www.ti.com/wireless

[22] (2005) ARM Secure SC200, smart card emulation development kit. ARM Limited, Inc. [Online]. Available: http://www.arm.com/

[23] (2005) User manual, SmartRF CC2420 ZigBee DK development. Chipcon AS. (Now Part of Texas Instruments). [Online]. Available: http://www.chipcon.com/
[24] (2001) ANSI X9.63, public key cryptography for the financial services industry: The elliptic curve key agreement and key transport protocols. National Institute of Standards and Technology. [Online]. Available: http://csrc.nist.gov
[25] J. A. Solinas, "Efficient arithmetic on koblitz curves," *Designs, Codes and Cryptography*, vol. 19, no. 2, pp. 195–249, Mar. 2000.
[26] D. Hankerson, J. L. Hernandez, and A. Menezes, "Software implementation of elliptic curve cryptography over binary fields," in *Proc. Cryptographic Hardware and Embedded Systems (CHES), LNCS Volume 1965*. Springer-Verlag, 2000, pp. 1–24.
[27] W. J. Dixon, "Analysis of extreme values," *Annals of Mathematical Statistics*, vol. 21, pp. 488–506, 1950.
[28] V. Barnett and T. Lewis, *Outliers in Statistical Data*. John Wiley & Sons, 1994.
[29] B. Efron, "Bootstrap methods: Another look at the jackknife," *Annals of Statistics*, vol. 7, pp. 1–26, 1979.
[30] B. Efron and R. J. Tibshirani, *An Introduction to the Bootstrap*. Chapman & Hall, 1993.
[31] F. Grubbs, "Procedures for detecting outlying observations in samples," *Technometrics*, vol. 11, no. 1, pp. 1–21, 1969.

**Caimu Tang** (S'97–M'05) received B.S. in Applied Mathematics from Xi'an Jiaotong University, Xi'an, China, in 1990, M.S. in Computer Science from Wayne State University, Detroit, Michigan, in 1997, and Ph.D. in Computer Science from University of Southern California, in 2005. From Aug. 2005 to April 2006, He was with Rockwell Scientific Company at Thousand Oaks, CA, as a research scientist. Since Aug. 2006, he has been with Tut Systems, Lake Oswego, Oregon, as a staff engineer. His research interests are in the areas of network security, video coding/transcoding, and wireless communications.

**Dapeng Oliver Wu** (S'98–M'04–SM'06) received B.E. in Electrical Engineering from Huazhong University of Science and Technology, Wuhan, China, in 1990, M.E. in Electrical Engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1997, and Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University, Pittsburgh, PA, in 2003. Since August 2003, he has been with Electrical and Computer Engineering Department at University of Florida, Gainesville, FL, as an Assistant Professor. His research interests are in the areas of networking, communications, multimedia, signal processing, and information and network security. He received the IEEE Circuits and Systems for Video Technology (CSVT) Transactions Best Paper Award for Year 2001, and the Best Paper Award in International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine) 2006. Currently, he serves as the Editor-in-Chief of *Journal of Advances in Multimedia*, and an Associate Editor for *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Circuits and Systems for Video Technology*, *IEEE Transactions on Vehicular Technology*, and the *International Journal of Ad Hoc and Ubiquitous Computing*. He is also a guest-editor for *IEEE Journal on Selected Areas in Communications* (JSAC), Special Issue on Cross-layer Optimized Wireless Multimedia Communications.