Integrating Continuous Credentials in Authentication Mechanisms

Dor Malka, Ittay Eyal

December 28, 2025

1 Abstract

Authentication is a fundamental aspect of security that can be viewed from two main perspectives: credentials and protocols. The credentials aspect is familiar to most of us through username and password, or OTPs used when accessing personal bank account or authenticating into services such as Google/Apple ID. While these discrete credentials, which rely on simply having or knowing something are widely used, there remains a largely unexplored space: continuous credentials.

Continuous credentials appear in several applications such as biometric authentication (fingerprints, eigenface or iris) and SSO mechanisms that rely on behavioral or environmental signals like GPS location etc. These credentials are not evaluated in a discrete way. Rather, they are measured by a mechanism that determines whether there are enough similarities above a predetermined threshold between an input and a stored figure.

These mechanisms introduce a spectrum of confidence instead of a strict yes or no decision. As achieving high security level based on one credential and satisfying the mechanism might be hard, we aim to study the integration of several continuous credentials. Our research will explore how multiple continuous credentials can be fused to form a robust authentication mechanism and determine an optimal mechanism, achieving high security level in wallet design for both digital and physical assets.

2 Related Work

Lin Hong et al. [1] found that automatic personal identification system based solely on fingerprints or faces is often not able to reach sufficiently low FAR and FRR. They integrated a biometric system which makes personal identification by integrating both faces and fingerprints operates during identification mode. The decision fusion of their system is designed to operate at measurement level, that is the system doesn't just output a single decision or label but rather a set of labels with confidence values. The system decision is based on the confidence of each one of the modules which might lead to a more reliable and informative overall confidence score.

These confidence values are characterized by the FAR values of the credential. The FAR values were calculated as the number of similarities between 2 measures above a threshold t. If there are 5 similarities out of 8 between 2 fingerprints and the threshold was 4, these 2 fingerprints will be considered equal.

Prabhakar et al. [2] examined the tradeoff between False Acceptance Rate (FAR) and False Rejection Rate (FRR), highlighting its impact on both the accuracy and security of biometric systems. Their findings suggest that most applications aim to operate at a point that balances these two metrics.

This concept is further developed by Sarkar et al. [3], who introduced it as the Equal Error Rate (EER). Sarkar defined this point as the operating point of the biometric system, emphasizing that the lower the EER value, the greater the performance of the biometric authentication system.

Eyal et al. [5] designed and formulated a foundational wallet model, defining four possible states for each credential – safe, loss, leak and theft. However, this work did not address the type of credentials involved, nor proposed a method to determine the probability of each credential's state.

3 Authentication Model

An authentication mechanism M is built on a set of credentials $\{c_1, c_2, \ldots, c_n\}$ and two players: a user U and an attacker A. Both players, try to satisfy the system with their own set of credentials $\{c_1, c_2, \ldots, c_n\}$ in order to reach the asset. Each credential c_i can be either discrete or continuously distributed. In this paper, we will focus on continuously distributed credentials. We will formalize the systems success and identify the optimal operating point for both single and multiple credentials.

3.1 Model Details

We follow the definitions given by Eyal [5]. A wallet w is defined by predicate of availability of N keys. Each key can be in one of the following states. Safe: only the user has access to the key. Loss: neither the user nor the attacker has access to the key. Leak: both the user and the attacker have access to the key. Theft: only the attacker has access to the key.

We define the probability associated with each state as follows: P_{safe}, P_{loss}, P_{leak} and P_{theft} corresponding respectively to the states of safe, loss, leak, and theft. Furthermore, the confidence associated with different decisions may be characterized by the genuine distribution and the impostor distribution, which are used to establish two error rates: false acceptance rate (FAR), which is defined as the probability of an impostor being accepted as a genuine individual and false rejection rate (FRR), which is defined as the probability of a genuine individual being rejected as an impostor.

A wallet w is comprised of a set of credentials $\{c_1, c_2, \ldots, c_n\}$ clasified as one of previously defined states.

Denoted S, i.e., $\{c_1, c_2, \ldots, c_n\} \in S = \{\text{safe}, \text{loss}, \text{leak}, \text{theft}\}$ the state of each credential. A scenario σ is defined as a vector of states of each credential in the wallet. Denote σ_i the state of credential c_i in scenario σ. An availability vector represents the availablity of all credentials to a user U or an attacker A. Denote by σ^U,σ^A the availability vector of the user and the attacker respectively.

In the following sections we will represent all continuously distributed credentials as the probability function of the matching score s denoted as $P_U[s]$. We follow the definitions given by Jain et al. [7] and generalize it to all continuously distributed credentials. If the stored reference template of the user U is represented by X_U and the acquired input for recognition is represented by X_Q then:

H_0 input X_Q does not come from the same person as the reference template X_U.

H_1 input X_Q comes from the same person as the reference template X_U.

D_O, D_1 are the imposter and geniuine persons trying to authenticate into the account. The matching score s, is usually a single number, that quantifies the similarity between an input X_Q and and the reference store template in the database X_U [2]. If the matching score $s(X_Q, X_U)$ is above a predetermined threshold t then decide D_1 else, decide D_0.

3.2 Single Credential

For a wallet w comprised of a single credential c_1, $w^{\text{single}}(c_1) = c_1$ we have built FAR vs FRR curves for Uniform, Parabolic and Gaussian probabilistic distribution functions and defined each one of the states as follows:

$$P_{\text{loss}} = \text{FRR} \cdot (1 - \text{FAR})$$

$$P_{\text{leak}} = \text{FAR} \cdot (1 - \text{FRR})$$

$$P_{\text{theft}} = \text{FRR} \cdot \text{FAR}$$

$$P_{\text{safe}} = 1 - \text{P}_{\text{loss}} - \text{P}_{\text{leak}} - \text{P}_{\text{theft}}$$

The probability for success of the wallet w, is defined as the probability of users successfully defend their wallets. In a single credential wallet, this is simply the probability that the key is neither theft, loss or leaked. i.e.,

$$P_{\text{success}}(w^{\text{single}}) = P_{\text{safe}}.$$

Until now, it has been common practice to select the operating point at the Equal Error Rate (EER), where FAR = FRR following Sarkar's claim: "The operating point is that point where the FAR is equal to the FRR and known as Equal Error Rate (EER)" [3]. Our findings indicate that a different operating point can yield a higher P_{safe}, thereby enhancing the system's overall security. Furthermore, We found that the operating point depends on the variance of the PDFs. We will further explore this in the following sections for different distributions.

3.2.1 Uniformly Distributed Credential

At first we analyzed the simple case of a single credential uniformly distributed. We defined two probability distribution functions (PDFs) for the user and the attacker, P_U and P_A respectively.

$$P_U(t) = \frac{1}{u_2 - u_1} \quad \text{for } u_1 \leq t \leq u_2$$

$$P_A(t) = \frac{1}{a_2 - a_1} \quad \text{for } a_1 \leq t \leq a_2$$

Where u_1, u_2 are the user PDFs' bounds and a_1, a_2 are the attacker PDFs' bounds.

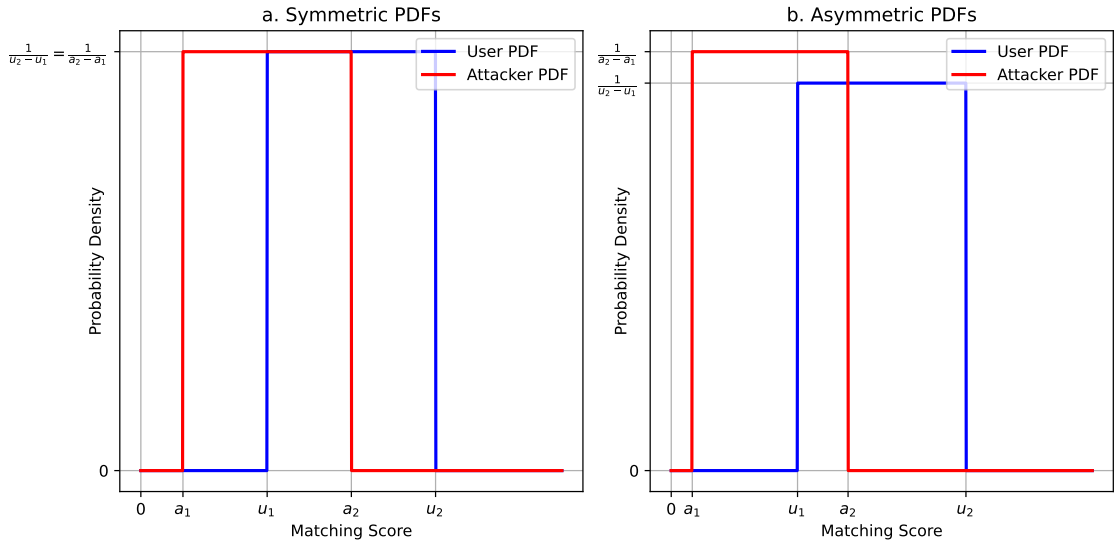

Figure 1: Symmetric and Asymmetric Uniform PDFs

We assume that $a_1 < u_1$ and $a_2 < u_2$ as the x axis represents the matching score s and higher values of s corresponds to the user D_1 as mentioned in the model details. Furthemore, we assume there is an overlaping region between the distributions; otherwise the scenario reduces to a trivial case. We also assume that the user and attacker PDFs are do not fully contain one another, as such cases would render them non-separable. Figure 1a illustrates the case where the user and attacker PDF's are symmetric, while Figure 1b illustrates asymmetric PDFs both as function of the matching score s. The probability of success for a single credential wallet is defined as:

$$P_{\text{success}}(w^{\text{single}}) = P_{\text{safe}} = 1 - \text{P}_{\text{loss}} - \text{P}_{\text{leak}} - \text{P}_{\text{theft}} = 1 - \text{FRR} - \text{FAR} + \text{FRR} \cdot \text{FAR}$$

Let T denote the threshold. Then the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are defined as:

$$\text{FAR}(T) = \int_T^{a_2} \frac{1}{a_2 - a_1} ds = \begin{cases} 1 & \text{if } T \leq a_1 \\ \frac{a_2 - T}{a_2 - a_1} & \text{if } a_1 < T \leq a_2 \\ 0 & \text{if } T > a_2 \end{cases}$$

$$\text{FRR}(T) = \int_{u_1}^{T} \frac{1}{u_2 - u_1} ds = \begin{cases} 0 & \text{if } T \leq u_1 \\ \frac{T - u_1}{u_2 - u_1} & \text{if } u_1 < T \leq u_2 \\ 1 & \text{if } T > u_2 \end{cases}$$

We defined the probability of success as a function of the threshold T by setting the $FAR(T)$

$FRR(T)$ into the equation and received:

$$P_{\text{success}}(T) = \begin{cases} 0 & \text{if } T \le a_1 \\ 1 - \frac{a_2 - T}{a_2 - a_1} & \text{if } a_1 < T \le u_1 \\ 1 - \frac{T - u_1}{u_2 - u_1} - \frac{a_2 - T}{a_2 - a_1} + \frac{T - u_1}{u_2 - u_1} \cdot \frac{a_2 - T}{a_2 - a_1} & \text{if } u_1 < T \le a_2 \\ 1 - \frac{T - u_1}{u_2 - u_1} & \text{if } a_2 < T \le u_2 \\ 0 & \text{if } T > u_2 \end{cases}$$

$P_{\text{success}}(T)$ is a continuous function in $[a_1, u_2]$,differentiable in (a_1, u_2) and maintains $P_{\text{success}}(a_1) = P_{\text{success}}(u_2)$ thus by Rolle's Theorem, there exists at least one point in (a_1, u_2) such that:

$$\frac{d}{dT} P_{\text{success}}(T) = 0.$$

The horizontal tangent point is:

$$T = \frac{a_1 + u_2}{2} \quad \text{for } u_1 \le T \le a_2$$

$$\frac{d}{dt} P_{\text{success}}(T) > 0, \text{ For every } T \in (u_1, \frac{a_1 + u_2}{2})$$

$$\frac{d}{dt} P_{\text{success}}(T) < 0, \text{ For every } T \in (\frac{a_1 + u_2}{2}, a_2)$$

Thus, by the First Derivative Test the maximum point is at $T = \frac{a_1 + u_2}{2}$.

$$P_{\text{success}}(T_{\text{opt}}) = \frac{(a_1 - u_2)^2}{4(a_1 - a_2)(u_1 - u_2)}$$

We calculated the EER point and showed it is not equal to the optimal point:

$$T_{\text{EER}} = \frac{a_1 \cdot u_1 - a_2 \cdot u_2}{a_1 - a_2 + u_1 - u_2} \neq \frac{a_1 + u_2}{2}$$

The maximum point represnents the optimal threshold of the wallet. By selecting the threshold value, we influnce the wallet's security sensetivity by adjusting the probability associated with each state in S. The optimal point indicates that increasing the offset between the two uniform distributions is likely to improve the wallet's success. This optimal point suggest an asymmetry between the user's and the attacker's distribution intervals.. Figure 2 illustrates the probability of success for a single credential wallet depends on the threshold T.

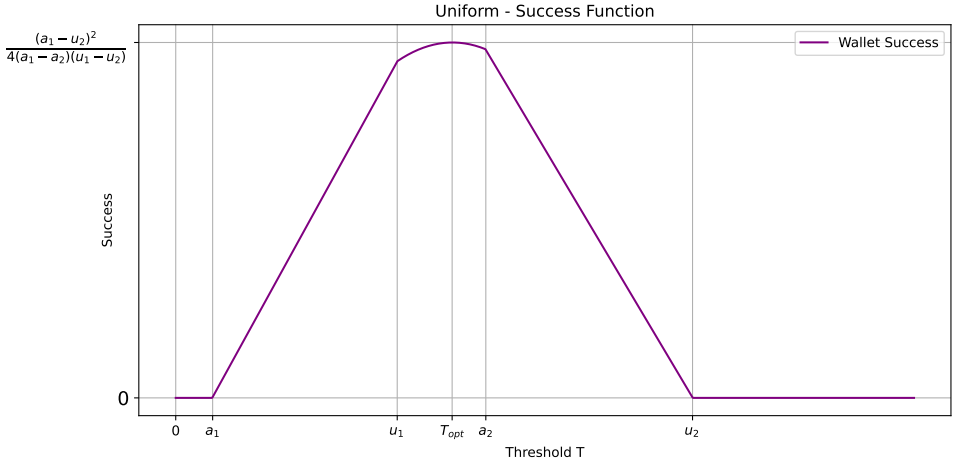

Figure 2: Probability of success for a single credential wallet asymmetric uniformly distributed

We can define the FAR and FRR at the optimal point as follows:

$$\mathrm{FAR}(T_{\mathrm{opt}}) = \frac{2a_2 - a_1 - u_2}{2(a_2 - a_1)}$$

$$\mathrm{FRR}(T_{\mathrm{opt}}) = \frac{a_1 + u_2 - 2u_1}{2(u_2 - u_1)}$$

Figure 3 illustrated the FAR vs FRR curve.

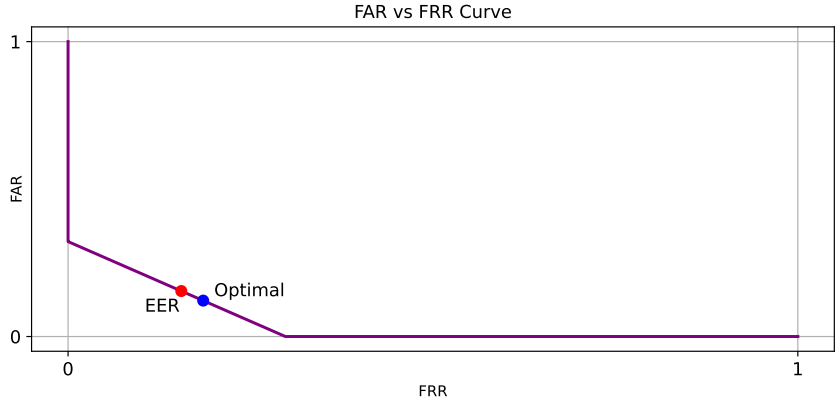

Figure 3: FAR vs FRR curve

3.2.2 Parabolic Distributed Credential

Our goal is to model credentials whose distributions closely resemble those observed in real measurement data. To this end, we analyze a parabolic probability distribution function, which provides

a flexible approximation of credential distributions that are often near-Gaussian. This choice is also consistent with the findings of Slobodan et al. on Eigenfinger and Eigenpalm feature distributions [6]. Accordingly, we define two probability density functions (PDFs) for the user and the attacker, denoted by P_U and P_A, respectively.

$$P_U(s) = \begin{cases} a \cdot s^2 + b \cdot s + c & \alpha_1 \leq s \leq \alpha_2 \\ 0 & s > \alpha_2 \vee s < \alpha_1 \end{cases}$$

$$P_A(s) = \begin{cases} d \cdot s^2 + e \cdot s + f & \beta_1 \leq s \leq \beta_2 \\ 0 & s > \beta_2 \vee s < \beta_1 \end{cases}$$

Here, a, b, c and d, e, f denote the parabolic coefficients of the user and attacker distributions, respectively. The parameters α_1, α_2 are the roots of the user's PDF, while β_1, β_2 are the roots of the attacker's PDF. Similarly, to the analysis of the uniform distribution, the x axis represents the matching score, such that higher values of score will be corrspondant to the reference template stored in the database X_U. If $\beta_2 < \alpha_1$, the two distributions do not overlap, and the problem becomes trivial. Conversely, if $\alpha_1 > \beta_1$ and $\beta_2 < \alpha_2$, the attacker's distribution is fully contained within the user's, resulting in a non-separable scenario. We therefore focus on the intermediate and most meaningful configuration, where

$$\beta_1 \leq \alpha_1 \leq \beta_2 \leq \alpha_2,$$

as illustrated in Figure 4.

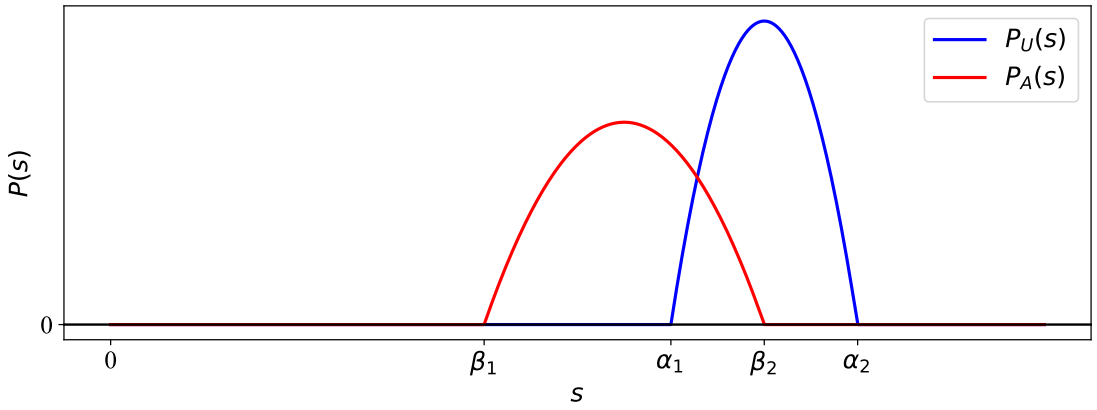

Figure 4: Parabolic PDFs

To reduce the degrees of freedom of the parabolic functions while maintaining a symbolic analysis, we express the coefficients directly in terms of their roots. Under the additional assumption that the integral of each PDF over its roots interval equals 1, the coefficients become fully determined. Accordingly, we define the coefficients as follows.

$$\alpha_1 \cdot \alpha_2 = \frac{c}{a} \rightarrow a = \frac{c}{\alpha_1 \cdot \alpha_2}$$

$$\alpha_1 + \alpha_2 = -\frac{b}{a} \rightarrow b = -\frac{c \cdot (\alpha_1 + \alpha_2)}{\alpha_1 \cdot \alpha_2}$$

$$\beta_1 \cdot \beta_2 = \frac{f}{d} \rightarrow d = \frac{f}{\beta_1 \cdot \beta_2}$$

$$\beta_1 + \beta_2 = -\frac{e}{d} \rightarrow e = -\frac{f \cdot (\beta_1 + \beta_2)}{\beta_1 \cdot \beta_2}$$

$$\int_{\alpha_1}^{\alpha_2} (a \cdot x^2 + b \cdot x + c) dx = 1 \Rightarrow c = \frac{6 \cdot \alpha_1 \cdot \alpha_2}{(\alpha_1 - \alpha_2)^3}$$

$$\int_{\beta_1}^{\beta_2} (d \cdot x^2 + e \cdot x + f) dx = 1 \Rightarrow f = \frac{6 \cdot \beta_1 \cdot \beta_2}{(\beta_1 - \beta_2)^3}$$

Therefore, we can write the parabolic PDFs as:

$$P_U(s) = \begin{cases} \frac{6}{(\alpha_1 - \alpha_2)^2} \cdot s^2 - \frac{6 \cdot (\alpha_1 + \alpha_2)}{(\alpha_1 - \alpha_2)^3} \cdot x + \frac{6 \cdot \alpha_1 \cdot \alpha_2}{(\alpha_1 - \alpha_2)^3} & \alpha_1 \leq x \leq \alpha_2 \\ 0 & x > \alpha_2 \vee x < \alpha_1 \end{cases}$$

$$P_A(s) = \begin{cases} \frac{6}{(\beta_1 - \beta_2)^2} \cdot x^2 - \frac{6 \cdot (\beta_1 + \beta_2)}{(\beta_1 - \beta_2)^3} \cdot x + \frac{6 \cdot \beta_1 \cdot \beta_2}{(\beta_1 - \beta_2)^3} & \beta_1 \leq x \leq \beta_2 \\ 0 & x > \beta_2 \vee x < \beta_1 \end{cases}$$

We will find FAR and FRR as a function of the threshold T and define the probability of success based on the single credential wallet as shown in Section 3.2:

$$\mathrm{FAR}(T) = \int_T^{\beta_2} P_A(s) ds = \begin{cases} 0 & T \leq \beta_1 \\ \frac{6\left(\frac{\beta_2^3}{3} - \frac{T^3}{3}\right)}{(\beta_1 - \beta_2)^3} - \frac{6\left(\frac{\beta_2^2}{2} - \frac{T^2}{2}\right)(\beta_1 + \beta_2)}{(\beta_1 - \beta_2)^3} + \frac{6\beta_1\beta_2(\beta_2 - T)}{(\beta_1 - \beta_2)^3} & \beta_1 < T \leq \beta_2 \\ 1 & T > \beta_2 \end{cases}$$

$$\mathrm{FRR}(T) = \int_{\alpha_1}^{T} P_U(s) ds = \begin{cases} 1 & T \leq \alpha_1 \\ \frac{6\left(\frac{T^3}{3} - \frac{\alpha_1^3}{3}\right)}{(\alpha_1 - \alpha_2)^3} - \frac{6\left(\frac{T^2}{2} - \frac{\alpha_1^2}{2}\right)(\alpha_1 + \alpha_2)}{(\alpha_1 - \alpha_2)^3} + \frac{6\alpha_1\alpha_2(T - \alpha_1)}{(\alpha_1 - \alpha_2)^3} & \alpha_1 < T \leq \alpha_2 \\ 0 & T > \alpha_2 \end{cases}$$

$$P_{\text{success}} = \begin{cases} 0 & T < \beta_1 \vee T > \alpha_2 \\ \frac{(T - \beta_1)^2 (2T + \beta_1 - 3\beta_2)}{(\beta_1 - \beta_2)^3} & \beta_1 \leq T \leq \alpha_1 \\ -\frac{(T - \alpha_2)^2 (T - \beta_1)^2 (2T - 3\alpha_1 + \alpha_2)(2T + \beta_1 - 3\beta_2)}{(\alpha_1 - \alpha_2)^3 (\beta_1 - \beta_2)^3} & \alpha_1 \leq T \leq \beta_2 \\ -\frac{(T - \alpha_2)^2 (2T - 3\alpha_1 + \alpha_2)}{(\alpha_1 - \alpha_2)^3} & \beta_2 \leq T \leq \alpha_2 \end{cases}$$

We differentiate $P_{\text{success}}(T)$ and compute its critical points in each interval. By comparing the stationary values obtained in all valid regions, we identify the global maximum, which corresponds to the optimal threshold T_{opt}.

Before writing the piecewise derivative, we define the polynomial coefficients:

$$
\begin{aligned}
q &= 4, \\
m &= -(5\alpha_1 + \alpha_2 + \beta_1 + 5\beta_2), \\
n &= \alpha_1(3\alpha_2 + \beta_1 + 6\beta_2) - \alpha_2^2 + \alpha_2\beta_2 - \beta_1^2 + 3\beta_1\beta_2, \\
\ell &= \alpha_1\big(\beta_1^2 - 3\beta_2(\alpha_2 + \beta_1)\big) + \alpha_2^2\beta_2.
\end{aligned}
$$

With these coefficients, the derivative of $P_{\text{success}}(T)$ is given by the following piecewise expression:

$$
\frac{dP_{\text{success}}}{dT} = \begin{cases}
0, & T < \beta_1 \ \vee \ T > \alpha_2, \\
\dfrac{6(T-\beta_1)(T-\beta_2)}{(\beta_1-\beta_2)^3}, & \beta_1 \le T \le \alpha_1, \\
-\dfrac{6(T-\alpha_2)(T-\beta_1)\big(qT^3 + mT^2 + nT + \ell\big)}{(\alpha_1-\alpha_2)^3(\beta_1-\beta_2)^3}, & \alpha_1 \le T \le \beta_2, \\
-\dfrac{6(T-\alpha_1)(T-\alpha_2)}{(\alpha_1-\alpha_2)^3}, & \beta_2 \le T \le \alpha_2.
\end{cases}
$$

In the second interval, the derivative has a single critical point at $T = \beta_1$. Since the derivative is strictly positive for all $T > \beta_1$, this point corresponds to a local minimum rather than a maximum. Similarly, in the fourth interval, the only critical point occurs at $T = \alpha_2$, and the derivative is strictly negative for all $T < \alpha_2$. Therefore, this interval also contains no maximum either.

We therefore turn to the third interval. In this region, the derivative is the product of a cubic polynomial and two linear factors. The linear factors vanish at $T = \beta_1$ and $T = \alpha_2$, both of which lie outside the third interval. Consequently, the existence of critical points within this interval depends solely on the cubic term. Solving this cubic ,reveals exactly one real root with the remaining two roots being complex. The closed form of the cubic solution can not be simplified further more than a complex expression. Thus, we denote the solution as T_{cubic}.

By examining the sign of the derivative on both sides of the critical point T_{cubic}, we verify that it constitutes a global maximum of $P_{\text{safe}}(T)$. We denote this maximizing point by T_{opt}.

To demonstrate that this optimal threshold differs from the Equal Error Rate (EER) threshold, we computed the EER point separately as follows:

$$
T_{\text{EER}} = \frac{\alpha_1\beta_1 - \alpha_2\beta_2}{\alpha_1 - \alpha_2 + \beta_1 - \beta_2} \neq T_{\text{opt}}
$$

We illustrate several user and attacker distributions and present their corresponding probability of success curves, expressed as functions of the threshold T in Figure 5 and Figure 6 respectively.

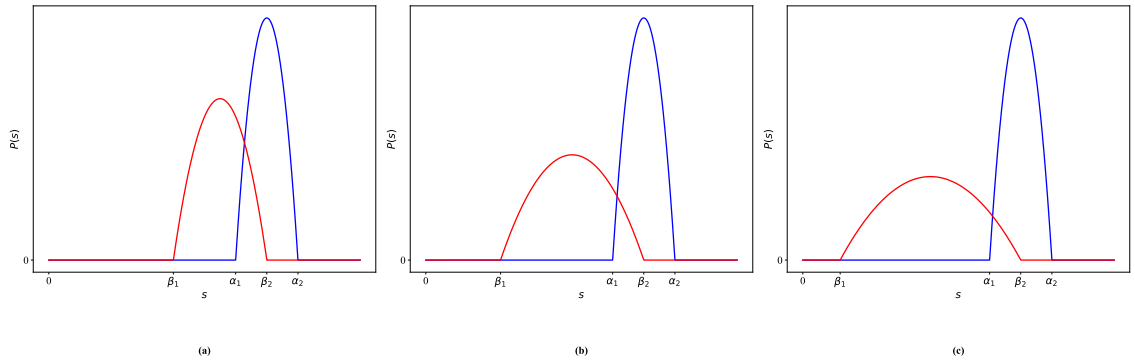

Figure 5: User and Attacker Parabolic Distributions

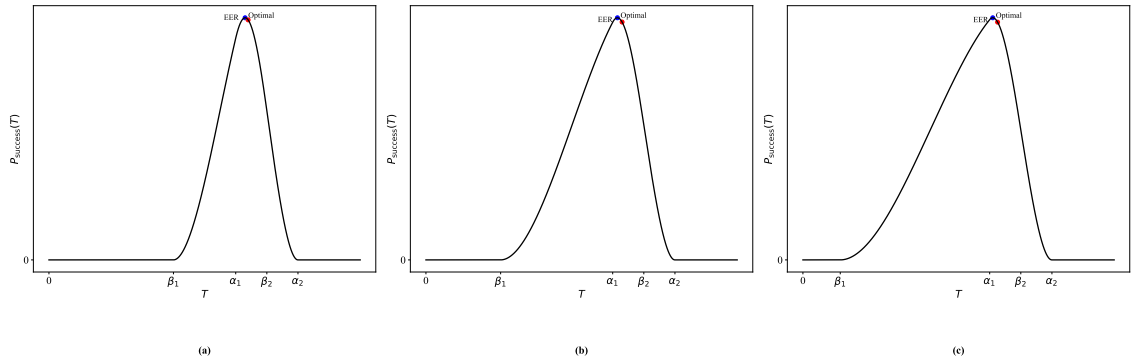

Figure 6: Probability of success for a single credential wallet parabolic distributed

Moreover, we illustrate the FAR–FRR curves for each pair of user and attacker distributions, and mark both the optimal point and the EER point, as shown in Figure 7.

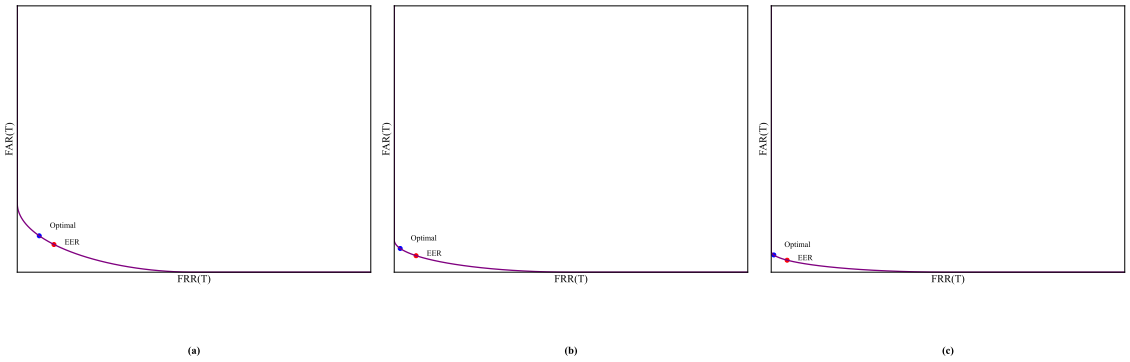

Figure 7: FAR vs FRR curve parabolic distributed

To quantify the effect of the variance on the deviation between the optimal operating point T_{opt} and the equal error rate (EER) point T_{EER}, we numerically computed this gap as a function of the attacker's variance. Decreasing the variance of the attacker achieved by reducing the distance between its roots, corresponds to reduced separability between the two distributions. The simulations reveal that as the variance increases, the gap $|T_{\text{opt}} - T_{\text{EER}}|$ grows accordingly, until the operating threshold moves into a regime where it effectively minimizes only one of the error rates, either FAR or FRR, driving the other to zero. This phenomenon is shown in Figure 8. These findings indicate that higher attacker variance enlarges the potential security advantage gained by operating at T_{opt} rather than at the EER point.

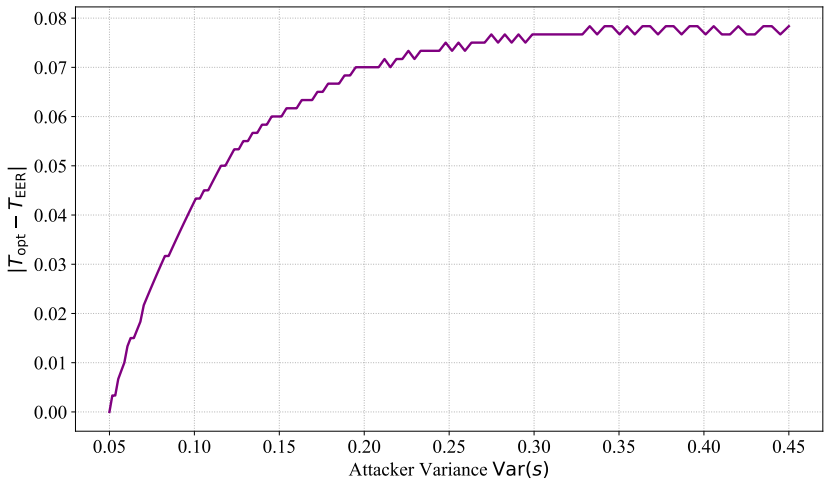

Figure 8: Gap between optimal point and EER point vs Variance of the attacker parabolic distributed

3.3 Two Credentials

For a wallet w comprised of two independently and identically distributed credentials, derived from either the same or different PDF's, we defined the integrated system success as the probability of users successfully defend their wallets under two scenarios:

a. **AND** Require both credentials to be satisfied. For success, we need both credentials to be either in safe state, or one in safe state and the other in leak state. If one of the credentials is either loss ot theft, the owner cannot satisfy the wallet and thus the wallet fails.

$$P_{\text{Success}}(w^{\text{AND}}) = \text{P}^1_{\text{safe}} \cdot \text{P}^2_{\text{safe}} + \text{P}^1_{\text{safe}} \cdot \text{P}^2_{\text{leak}} + \text{P}^2_{\text{safe}} \cdot \text{P}^1_{\text{leak}} \tag{1}$$

b. **OR** Require at least one credential to be satisfied. For success, we need both credential to be either in safe state, or one in safe state and the other in loss state. If one of the credentials is either leak ot theft, the attacker can satisfy the wallet and thus the wallet fails.

$$P_{\text{Success}}(w^{\text{OR}}) = \text{P}^1_{\text{safe}} \cdot \text{P}^2_{\text{safe}} + \text{P}^1_{\text{safe}} \cdot \text{P}^2_{\text{loss}} + \text{P}^2_{\text{safe}} \cdot \text{P}^1_{\text{loss}} \tag{2}$$

For each wallet type, we analyzed the case of two independently and identically distributed credentials in 2 cases:

a. A mechanism comprised of 1 discrete credential and 1 continuous credetial.

b. A mechanism comprised of 2 continuously distributed credentials

We derived the optimal operating point for both **AND** and **OR** wallets by maximizing the respective success probabilities with respect to the thresholds of each credential.

3.4 1 Discrete and 1 Continuous Credential

We started by analyzing the case of an **AND** wallet comprised of 1 discrete credential and 1 continuous credential. Denote s_i the state of credential $i \in (Discrete, Continuous)$, we defined the discrete credential with a constant value of each one of the probabilities' states as: $P^1_{safe}, P^1_{loss}, P^1_{leak}, P^1_{theft}$ corrsponding respectively to each one of the states: safe, loss, leak and theft. The continuous credential is defined by its PDFs for the user and the attacker, P_U and P_A respectively. We firstly analyzed the uniformly distributed credential between the bounds of u_1,u_2 corrsponding to the user distribution and a_1,a_2 corresponds to the attacker, similarly to Section 3.2.1. We derived the probability of the continuous credentail as follows:

$$\begin{aligned} P^2_{safe} &= 1 - \text{FAR}(T) - \text{FRR}(T) + \text{FAR}(T) \cdot \text{FRR}(T), \\ P^2_{leak} &= \text{FAR}(T)\big(1 - \text{FRR}(T)\big). \end{aligned}$$

To analyze the probability of success for the **AND** wallet, we set the above probabilities into Equation 1. Thus, the probability of success is a function of the threshold T and divided into 5 intervals.

$$P_{\text{success}}(T) = \begin{cases} P^1_{\text{safe}}, & T \le a_1, \\ (P^1_{\text{safe}} + P^1_{\text{leak}}) - P^1_{\text{leak}} \dfrac{a_2 - T}{a_2 - a_1}, & a_1 < T \le u_1, \\ \dfrac{u_2 - T}{u_2 - u_1} \left[(P^1_{\text{safe}} + P^1_{\text{leak}}) - P^1_{\text{leak}} \dfrac{a_2 - T}{a_2 - a_1} \right], & u_1 < T \le a_2, \\ \dfrac{u_2 - T}{u_2 - u_1} (P^1_{\text{safe}} + P^1_{\text{leak}}), & a_2 < T \le u_2, \\ 0, & T > u_2 \end{cases}$$

We analyze the success probability $P_{\text{success}}(T)$ by partitioning the threshold domain into five intervals, each corresponding to a distinct relative positioning of the threshold with respect to the attacker and user distributions.

The first interval, $T \le a_1$, corresponds to the case in which the threshold is lower than the minimum value of the attacker distribution. In this regime, the FAR is equal to 1, while the FRR is equal to 0. Consequently, the safe probability of the continuous credential is zero, and the success probability converges to P^1_{safe}. Since P^1_{safe} is constant in this interval, no interior maximum exists.

The second interval, $a_1 < T \le u_1$, corresponds to the case in which the threshold lies between the minimum value of the attacker distribution and the minimum value of the user distribution. In this region, the FAR decreases linearly as a function of T, while the FRR remains equal to 0. As a result, the probabilities of the safe state and the leak state of the continuous credential are $1 - \text{FAR}(T)$ and $\text{FAR}(T)$, respectively. In this interval, $P_{\text{success}}(T)$ is a strictly increasing function, as its derivative is a constant positive value, and therefore the maximum is attained at the boundary point

$$T_{\text{opt2}} = u_1.$$

The third interval, $u_1 < T \le a_2$, corresponds to the case in which the threshold lies between the minimum value of the user distribution and the maximum value of the attacker distribution. In this region, both FAR and FRR vary linearly with T, resulting in a success probability that is quadratic as a function of T. Differentiating $P_{\text{success}}(T)$ yields a single critical point inside the interval,

$$T_{\text{opt3}} = \frac{u_2 + a_2 - (a_2 - a_1) \dfrac{P^1_{\text{safe}} + P^1_{\text{leak}}}{P^1_{\text{leak}}}}{2}$$

By examining the optimal point in this interval, we can deduce that as the variance of the attacker distribution increases, the optimal threshold T_{opt3} shifts toward the lower boundry of the interval, u_1. Moreover, for a discrete credential with high safe values P^1_{safe}, and low leak values P^1_{leak}, the optimal threshold shifts toward the lower boundary as well. Thus, in such case, the success of the wallet becomes mainly dependent on the discrete credential. Conversely, a discrete credential with high leak values P^1_{leak} and low safe values P^1_{safe} causes the optimal threshold to shift toward the upper boundary of the interval, a_2. In this scenario, the success of the wallet relies more heavily on the continuous credential.

The fourth interval, $a_2 < T \le u_2$, corresponds to the case in which the threshold exceeds the maximum value of the attacker distribution. In this regime, the FAR is equal to 0, while the FRR

increases linearly with T. Consequently, $P_{\text{success}}(T)$ is a strictly decreasing function in this interval, and the maximum is attained at the boundary point

$$T_{\text{opt4}} = a_2.$$

Finally, the fifth interval, $T > u_2$, corresponds to the case in which the threshold exceeds the maximum value of the user and the attacker distributions, leaving the success probability equal to 0.

To determine the global optimal operating point, we compare all stationary points and boundary maxima obtained in the valid intervals. The optimal threshold is achieved in the third interval, where the attacker and user distributions overlap and the success function attains an interior maximum. Substituting $T_{\text{opt}} = T_{\text{opt3}}$ into $P_{\text{success}}(T)$ yields

$$P_{\text{success}}(T_{\text{opt}}) = \frac{\left(-a_1\left(P^1_{\text{safe}} + P^1_{\text{leak}}\right) + a_2 P^1_{\text{safe}} + P^1_{\text{leak}}\, u_2\right)^2}{4P^1_{\text{leak}}(a_2 - a_1)(u_2 - u_1)}.$$

We have done similar analysis for the **OR** wallet. We defined the credentials' probabilities of the wallet as follows:

$$\begin{aligned}
P_{\text{safe1}} &= 1 - \text{FAR}(T) - \text{FRR}(T) + \text{FAR}(T) \cdot \text{FRR}(T),\\
P_{\text{safe2}} &= k_1,\\
P_{\text{loss1}} &= \text{FRR}(T)\left(1 - \text{FAR}(T)\right),\\
P_{\text{loss2}} &= k_2.
\end{aligned}$$

Therefore, the probability of success for the **OR** wallet is defined as:

$$P_{\text{success}}(T) = \begin{cases}
0, & T \le a_1,\\
\dfrac{T - a_1}{a_2 - a_1}\,(k_1 + k_2), & a_1 < T \le u_1,\\
\dfrac{T - a_1}{a_2 - a_1}\left[k_1 + k_2 - k_2\,\dfrac{T - u_1}{u_2 - u_1}\right], & u_1 < T \le a_2,\\
k_1 + k_2 - k_2\,\dfrac{T - u_1}{u_2 - u_1}, & a_2 < T \le u_2,\\
k_1, & T > u_2.
\end{cases}$$

By differentiating every interval and identifying the critical points, we found that the optimal threshold that leads to the maximum probability of success lies in the third interval where $u_1 < T \le a_2$ and is given by:

$$T_{\text{opt}} = \frac{a_1 k_2 + u_2(k_1 + k_2) - k_1 u_1}{2k_2}$$

And the maximum probability of success at this point is:

$$P_{\text{success}}(T_{\text{opt}}) = \frac{\left(a_1 k_2 - u_2(k_1 + k_2) + k_1 u_1\right)^2}{4k_2(a_2 - a_1)(u_2 - u_1)}$$

For both wallet types, we observed that the optimal operating point T_{opt} differs from the equal error rate (EER) point T_{EER}. As the EER depends on the PDF's type solely, we calculated the EER point and showed each wallet's success in Figure 9 and Figure 10 respectively.

$$T_{\text{EER}} = \frac{a_1 u_1 - a_2 u_2}{a_1 - a_2 + u_1 - u_2}$$

4 Model

4.1 Mechanism Success 2 credentials

4.2 Mechanism Success 3 credentials

5 Optimal Mechanism

6 Conclusion

References

[1] Lin Hong and Anil Jain. *Integrating Faces and Fingerprints for Personal Identification.* IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998.

[2] S. Prabhakar, S. Pankanti, and A. K. Jain. *Biometric recognition: Security and privacy concerns.* IEEE Security & Privacy, 1(2), 33–42, 2003.

[3] Arpita Sarkar and Binod K. Singh. *A review on performance, security and various biometric template protection schemes for biometric authentication systems.* Multimedia Tools and Applications, vol. 79, nos. 37–38, pp. 27721–27776, Oct. 2020.

[4] Marwa Mouallem and Ittay Eyal. *Asynchronous Authentication.* CCS 2024 - Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security, pp. 3257–3271.

[5] Ittay Eyal. *On cryptocurrency wallet design..* Cryptology ePrint Archive, Paper 2021/1522,2021. https://eprint.iacr.org/2021/1522.

[6] Slobodan Ribaric and Ivan Fratric. *A Biometric Identification System Based on Eigenpalm and Eigenfinger Features.* IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume: 27, Issue: 11, November 2005.

[7] Anil K. Jain, Arun Ross and Salil Prabhakar. *An introduction to biometric recognition.* IEEE Transactions on Circuits and Systems for Video Technology, Volume: 14, Issue: 1, January 2004.