*Entropy* **2015**, *17*, 3806-3837; doi:10.3390/e17063806

OPEN ACCESS
*entropy*
ISSN 1099-4300
www.mdpi.com/journal/entropy

*Article*

# On the Detection of Fake Certificates via Attribute Correlation

**Xiaojing Gu * and Xingsheng Gu**

Key Laboratory of Advanced Control and Optimization for Chemical Process, Ministry of Education, East China University of Science and Technology, 200237 Shanghai, China

* Author to whom correspondence should be addressed; E-Mail: xjing.gu@ecust.edu.cn; Tel.: +86-21-67792401.

Academic Editor: Antonio M. Scarfone

*Received: 14 November 2014 / Accepted: 1 June 2015 / Published: 8 June 2015*

---

**Abstract:** Transport Layer Security (TLS) and its predecessor, SSL, are important cryptographic protocol suites on the Internet. They both implement public key certificates and rely on a group of trusted certificate authorities (*i.e.*, CAs) for peer authentication. Unfortunately, the most recent research reveals that, if any one of the pre-trusted CAs is compromised, fake certificates can be issued to intercept the corresponding SSL/TLS connections. This security vulnerability leads to catastrophic impacts on SSL/TLS-based HTTPS, which is the underlying protocol to provide secure web services for e-commerce, e-mails, *etc*. To address this problem, we design an attribute dependency-based detection mechanism, called SSLight. SSLight can expose fake certificates by checking whether the certificates contain some attribute dependencies rarely occurring in legitimate samples. We conduct extensive experiments to evaluate SSLight and successfully confirm that SSLight can detect the vast majority of fake certificates issued from any trusted CAs if they are compromised. As a real-world example, we also implement SSLight as a Firefox add-on and examine its capability of exposing existent fake certificates from DigiNotar and Comodo, both of which have made a giant impact around the world.

**Keywords:** certification; man-in-the-middle attacks; attribute correlation

---

## 1. Introduction

Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are built upon an X.509 public key infrastructure [1] and used as a base in important secure protocols and applications on the Internet, such as HTTPS, VPN and SMTPS . Within an X.509 infrastructure, certificate authorities (CAs) are in charge of checking other entities' identity and issuing X.509 certificates to verified entities, which may be another CA or end entity. The root CAs issue certificates to themselves, and the certificates of intermediate CAs are issued from other CAs. As a result, any end entity's certificate can be chained back to a root CA certificate through zero or several intermediate CA certificates, which form a certification path [1]. SSL/TLS employ end entity certificates to authenticate peer identities [2,3]. In particular, the end entity obtains a legitimate identity if its certificate can be chained back to a trusted CA along its certification path. The X.509 public key infrastructure also defines necessary fields and syntax present in X.509 certificates [2]. In this paper, we refer to the fields as attributes.

HTTPS uses SSL/TLS to encrypt HTTP connections, thus providing secure web services to a range of web applications, including online business, finance, healthcare, mailing services, and so on. In HTTPS connections, browsers authenticate web server identities based on a group of pre-agreed root and intermediate CAs. This validation process basically depends on two requirements. One is whether the web server's certificate is issued by one of the trusted CAs. The other is whether the certificate's common name (*i.e.*, CN) is bound to the web server's domain name. If both requirements are fulfilled, browsers confirm this web server's identity as legitimate. Otherwise, an alert will be displayed to make users aware that the certificate may be fake, and the web access is held immediately to prevent any potential attacks.

However, if one of the trusted CAs is compromised, fake certificates can be issued and used to hijack targeted HTTPS connections [4,5]. Browsers are not aware of the underlying attacks launched by this kind of fake certificate, because they trust the compromised CA by default and cannot distinguish which trusted CA is the legal one to issue which certificate. As reported from the SSL Observatory project [6], there are more than 600 certificate authorities that browsers should trust by default [7]. As a result, attackers are only required to compromise one of these CAs, which they are capable of breaking into. Such a threat consequently forces mainstream browsers to revoke their trust on these compromised CAs that have been discovered, such as DigiNotar [8–10] and Comodo [11]. However, this temporary countermeasure is followed by a side effect that browsers no longer trust the legitimate certificates that were already issued from DigiNotar and Comodo, as well. To make things worse, browsers lose the chance to withdraw their trust of the compromised CAs if they are not discovered.

To address these problems, online detection systems, such as Perspectives [12], HTTPS Everywhere [13] and Google Certificate Catalog [14], have been proposed. They conduct a direct bit-to-bit comparison between the examined certificate and its legitimate sample obtained from the Internet. As these systems check certificate identities on-line, attackers, who can use fake certificates to hijack users' HTTPS tunnels, are more likely to be able to intercept or block the corresponding connections to these on-line services, as well. The Sovereign Keys Project [15], on the other hand, provides a systematic solution for this structural insecurity. However, the implementation of sovereign

keys involves cooperation among different CAs and web/DNS servers, thus making it hard to be practically deployed.

In this paper, we propose SSLight, an attribute dependency-based detection mechanism, to help browsers identify fake certificates issued from compromised CAs. SSLight basically relies on a probabilistic model built on a set of legitimate samples. Fake certificates thus can be detected as dependencies between some of their attributes that rarely occur among the legitimate samples. For example, as Australian CAs have never signed any legitimate certificates to American servers, a certificate is more likely to be a fake one if it is issued by an Australian CA, but possessed by an American server. As a result, SSLight is capable of exposing fake certificates from compromised CAs, even if they are not discovered, and mitigating the false alarm on legitimate certificates, as well. SSLight does not require instant on-line checking, helping it circumvent potential network interceptions. Moreover, SSLight is a lightweight solution that does not need cooperation from remote servers or CAs.

In sum, we have made three contributions in this paper.

1. We have designed SSLight, a novel attribute dependency-based detection mechanism, to enhance SSL/TLS's authentication. SSLight is capable of exposing fake certificates issued from trusted, but compromised, CAs.

2. SSLight is built on a training set with 830,306 legitimate certificate samples. We have conducted extensive experiments to evaluate SSLight's detection capability. The experimental results show that SSLight can detect the vast majority of fake certificates issued from any compromised CA with a relatively low false positive rate.

3. We have implemented SSLight as a Firefox add-on and use it to detect real-world fake certificates from DigiNotar and Comodo, both of which have made a catastrophic impact around the world. SSLight achieves a relatively high detection rate on these real-world examples.

The remainder of the paper is organized as follows. Section 2 explains the attributes and the attribute dependency in X.509 certificates. Section 3 presents the threat model. Section 4 elaborates on the design of SSLight. In Section 5, SSLight is thoroughly evaluated and implemented as a Firefox add-on to examine real-world examples. Before concluding this paper, in Section 8, we discuss the limitations of our proposal in Section 6 and review related works in Section 7.

## 2. Background

This section presents the details of the attributes in X.509 certificates and the concept of attribute dependency.

### *2.1. Attributes in X.509 Certificates*

SSL/TLS employ the X.509 v3 certificate format to profile their X.509 certificates with necessary fields, called attributes, and corresponding usages [2]. These attributes can be classified into two groups, basic certificate attributes and certificate extension attributes [2], both of which are encoded following the ASN.1 distinguished encoding rules (DER) [16] in order to facilitate signature calculation.

Basic certificate attributes contain basic information related to the owner and its issuer. In particular, two basic certificate attributes, *Subject* and *Issuer* , include several sub-fields defined in the X.500 specification [17]. In this paper, we refer to these sub-fields as attributes, too. Certificate extension attributes, on the other hand, associate additional information with the owner and for managing relationships between CAs [2].

To receive a valid certificate, an entity, maybe a CA or a web server in this paper, first uses its private key to generate a certificate signing request (CSR) [18]. This CSR is subsequently sent to a trustworthy organization, actually another CA, for validation. After checking the entity's identity, the organization issues a signed certificate back to the requested entity. This issuing process always involves human interactions to fill in the certificate's attributes with necessary personal information. For example, if the entity is a CA located in America, the attribute *CA* and *Country* should be set to *TRUE* and *US*, respectively. As the contents in any attribute are involved in the signature calculation, they cannot be changed when the certificate is already signed. Any certificate is located in a certification path, in which an end entity certificate can be traced back to a root CA certificate through zero or several intermediate CA certificates [1]. From the bottom to the top of each certification path, the upper certificate is owned by a CA, which uses a private key to sign a lower certificate, and the top-most CA signs its certificate itself. With this signing chain, the trust assigned to the top-most certificate can be propagated to the bottom one. In this way, the browsers can only install hundreds of CA certificates and then trust billions of web sites later.

The left side of Figure 1 shows an example of a Google certificate. It is an end entity certificate and includes 15 basic certificate attributes, in which five belong to *Subject* attributes, three are *Issuer* attributes and five are certificate extension attributes. We observe much information from these attributes, like: the certificate's valid period is from the 18 December 2009 to 2011; the public key algorithm is RSA; the key length is 1024 bits; it is an American certificate, but issued by a South Africa CA, *etc*. In this paper, we assume the attributes that have not appeared in a certificate contain an empty value by default. The right side of this figure shows the corresponding certification path in which the Google certificate is located. The root CA, Verisign Class 3, issues a CA certificate to an intermediate CA, Thawte SGC , which signs the end entity certificate to Google.

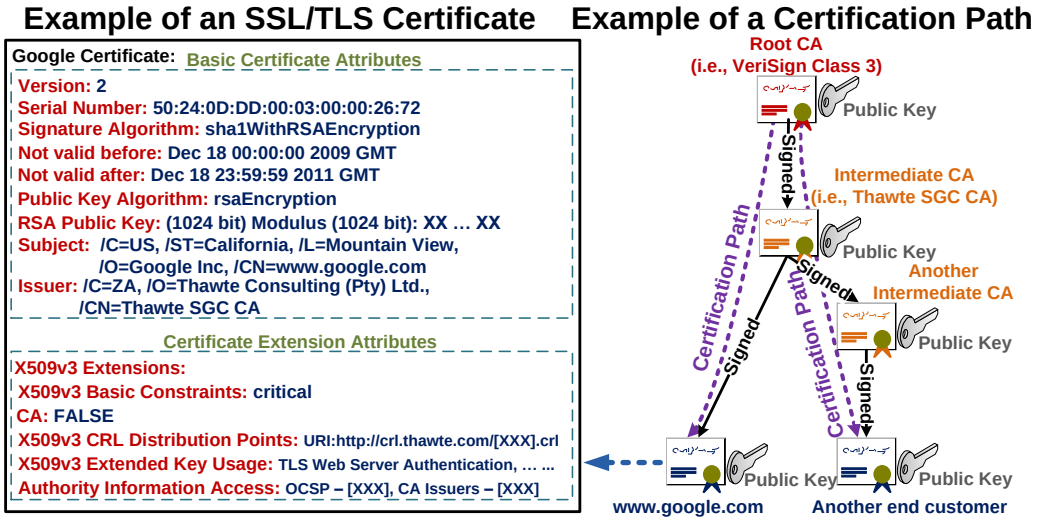
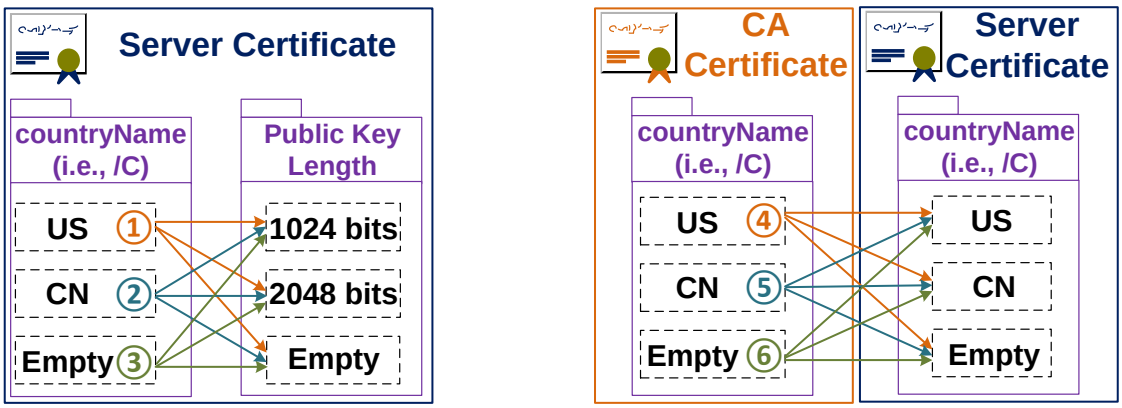



**Figure 1.** An SSL/Transport Layer Security (TLS) certificate with a certification path.

### *2.2. Attribute Dependency*

We define attribute dependency as the conditional probability distribution for all of the possible values of an attribute given a certain value in another attribute (the formalized definition is presented in Equation (5) in Section 4.1). These conditional probabilities can be calculated based on a set of legitimate certificates. According to whether the two attributes are from the same certificate or different certificates along with a certification path, we group attribute dependencies into two types, certificate attribute dependency and certification path attribute dependency. As a certificate's *Issuer* attributes indicate its issuer's *Subject* attributes along with a certification path, the dependency between an *Issuer* attribute and another attribute in the same certificate can be considered as a certification path attribute dependency. The certificate attribute dependency represents the relationship inside a certificate, while the certification path attribute dependency reflects the relationship between two different certificates from the same certification path.

Figure 2a illustrates an example for the certificate attribute dependency. Two attributes, *countryName* and *Public Key Length*, in a server certificate are considered. The *countryName* is assumed to have possible values *US*, *CN* and *Empty* , while the *Public Key Length* includes *1024*, *2048* and *Empty*. Each arrow line indicates a conditional probability for a value of the attribute *Public Key Length* given a certain value in the *countryName*. We observe three certificate attribute dependencies, ①, ② and ③, in which the certain value of the *countryName* is *US*, *CN* and *Empty*, respectively. Figure 2b, on the other hand, shows an instance of the certification path attribute dependency between the attribute *countryName* in a server certificate and a CA certificate, both of which are located at the same certification path. The two *countryName* attributes are assumed to possess possible values *US*, *CN* and *Empty*. As can be seen, there are three certification path attribute dependencies, ④, ⑤ and ⑥.




(a) (b)

**Figure 2.** Tow different types of attribute dependency. (**a**) Certificate attribute dependency; (**b**) certification path attribute dependency.

## 3. Threat Model

Figure 3 demonstrates the security threat involved in this paper using the real-world compromised CAs, DigiNotar and Comodo. We use Firefox Version 5.0.1 for this demonstration, because Firefox has announced withdrawing its trust in DigiNotar and Comodo since Version 6.0.1 [11,19,20]. Since

we cannot compromise the real DigiNotar and Comodo, we set up two private CAs in our laboratory to impersonate them instead. We then add the two private CA certificates into the trusted authorities list in Firefox; thus, they can be used as the real compromised DigiNotar and Comodo. To hijack HTTPS connections to the Google mail service, we deploy a man-in-the-middle SSL proxy [21] with fake Google certificates in our laboratory and configured Firefox to access HTTPS sessions through this proxy by default. As shown in Figure 3a, the legitimate Google certificate issued by Thawte SGC CA has been accepted by Firefox. However, Figure 3a,b demonstrates that Firefox also accepts fake Google certificates from DigiNotar and Comodo by default. As a result, users are not aware of underlying attacks when they access Gmail through HTTPS connections, and their account information will be leaked. Note that we obtain the same results in other major browsers, such as IE and Chrome.

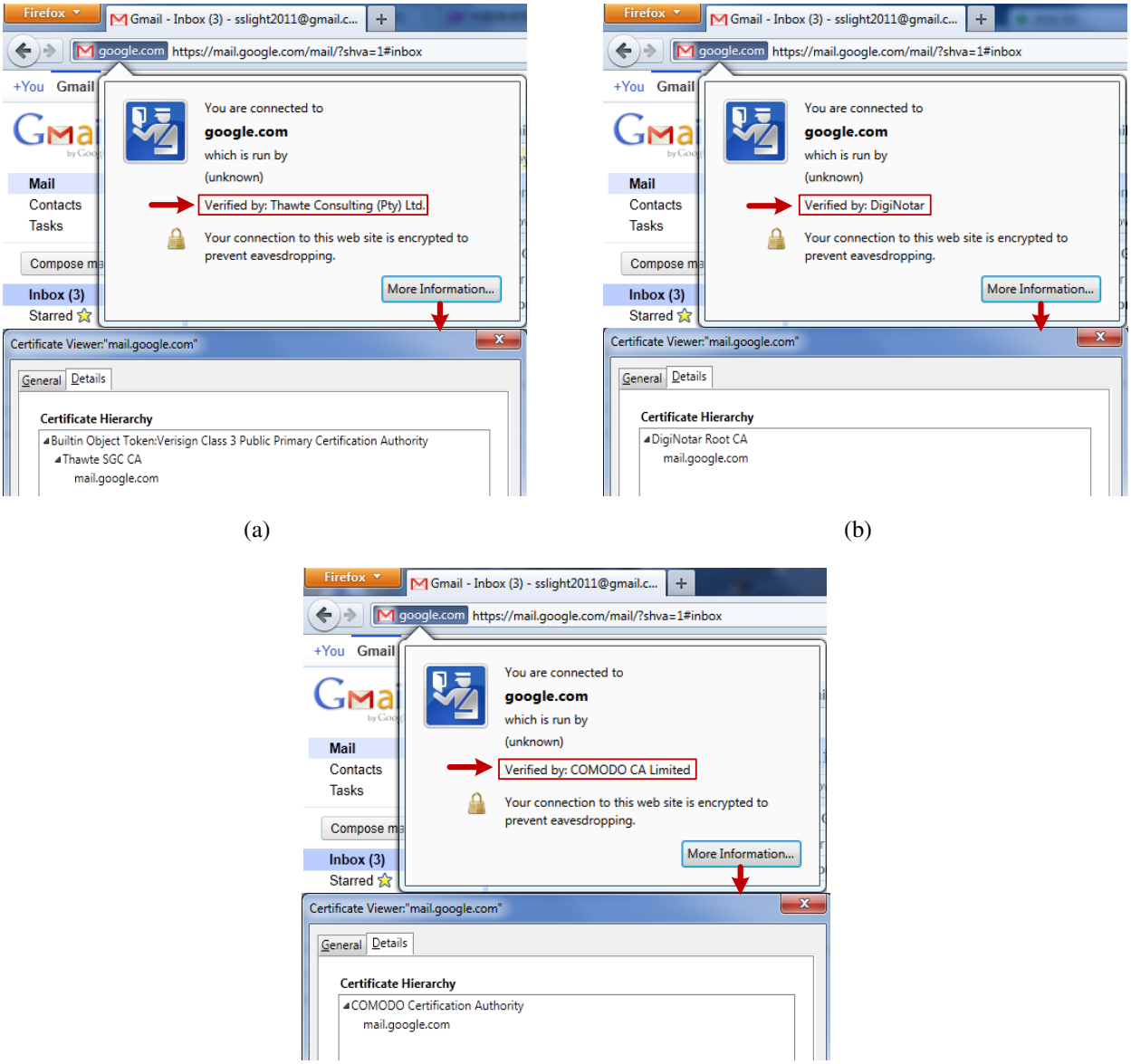



**Figure 3.** Both the legitimate and fake mail.google.com certificates have been accepted by Firefox (Version 5.0.1). (**a**) Legitimate certificate issued by Thawte; (**b**) fake certificate issued by DigiNotar; (**c**) fake certificate issued by Comodo.

In this paper, attackers are assumed to be able to intrude any CAs trusted by browsers and hijack any connections to and from the browsers. Note that attackers cannot modify the attributes in any trusted CA certificate because the CA certificates are pre-installed in browsers. Although attackers can exploit the compromised CA to issue fake certificates with arbitrary attributes, SSLight, or human beings, can easily detect these naive fake certificates through certificate attribute dependency. In this case, sophisticated attackers duplicate attributes from the legitimate certificate to its corresponding fake one, thus circumventing this kind of detection. Moreover, as sophisticated attackers can use the compromised CA to issue any number of intermediate CAs with arbitrary attributes, the detection based on the dependency between attributes from different CA certificates in the same certification path can be easily evaded. In this paper, SSLight focuses on the usage of the dependency between attributes from the server certificate and any of its CA certificates along with the same certification path to be against sophisticated attackers who:

- cannot do any modification in the trusted CA certificates;
- can duplicate attributes from legitimate certificates to the corresponding fake ones;
- can issue any number of intermediate CAs with arbitrary attributes using the trusted, but compromised, CA;
- can hijack or block any connections to and from the browsers.

The last item indicates that SSLight can work under the worst network conditions, in which any information from the Internet may be faked.

## 4. SSLight

In this section, we first build up a probabilistic model based on attribute dependencies among legitimate samples and then elaborate on the design of SSLight on top of this model. As a consequence, we introduce two factors, attack range reduction and false positive, to evaluate SSLight's detection capability.

### *4.1. Probabilistic Model*

Let a web server $q$'s legitimate certificate be $C_q^1$, which is associated with a certification path, defined as:

$$\Gamma(C_q^1) = \{C_q^i,\ i \in [1, N_q]\}, \tag{1}$$

where $N_q = ||\Gamma(C_q^1)||$ is the depth of the path $\Gamma(C_q^1)$. $C_q^i \in \Gamma(C_q^1)$ represents the $i$-th level certificate and $C_q^{i+1}$ issues $C_q^i$ when $i \in [1, N_q - 1]$. Hence, $C_q^1$ is a server certificate, and $C_q^{N_q}$ is a root CA certificate that is self-signed. Other $C_q^i,\ i \in [2, N_q - 1]$ are intermediate CA certificates along with the certification path.

**Proposition 1.** *Even if $C_{q_1}^{i>1} \in \Gamma(C_{q_1}^1)$ and $C_{q_2}^{i>1} \in \Gamma(C_{q_2}^1)$, where $\Gamma(C_{q_1}^1) \neq \Gamma(C_{q_2}^1)$, we may still have $C_{q_1}^{i>1} = C_{q_2}^{i>1}$, because the same CA can issue certificates to different entities.*

Based on Equation (1), we thus define a non-empty training set including legitimate certificate samples as:

$$\mathbb{C} = \{\Gamma(C_q^1),\ q \in [1, Q]\}, \tag{2}$$

where $Q = ||\mathbb{C}||$ is the size of the legitimate sample set $\mathbb{C}$. In this paper, we assume that browsers pre-agree to trust $\forall C_q^{i>1} \in \mathbb{C}$ and cannot trust $C_e^{i>1} \notin \mathbb{C}$.

In $\mathbb{C}$, we use $N_{max} = \underset{\Gamma(C_q^1)\in\mathbb{C}}{max} ||\Gamma(C_q^1)||$ to represent the maximum certification path depth. Let $\mathbb{A}^i = \{A_j^i\}$ for $\forall i \in [1, N_{max}]$ be the set of considered attributes in the $i$-th level certificate, and $||\mathbb{A}^i||$ is the size of set $\mathbb{A}^i$. For $\forall A_j^i \in \mathbb{A}^i$, $\mathbb{V}_j^i = \{V_k^{j,i}\}$ is the set of values that attribute $A_j^i$ may take, and $||\mathbb{V}_j^i||$ represents the number of these possible values. As a consequence, we define the subset $\mathbb{C}(i, j, k) \subseteq \mathbb{C}$ to include certification paths $\Gamma(C_q^1)$ in which the value of $A_j^i$, denoted as $A_j^{i,q}$, is set to $V_k^{j,i}$ as:

$$\mathbb{C}(i, j, k) = \{\Gamma(C_q^1) \in \mathbb{C},\ if\ V(A_j^{i,q}) = V_k^{j,i}\}, \tag{3}$$

where $V(A_j^{i,q}) \in \mathbb{V}_j^i$ represents the value assigned to $A_j^{i,q}$.

With the help of Equation (3), we calculate the probability of the certification paths $\Gamma(C_q^1)$ whose $V(A_{j=J_x}^{i=I_x,q}) = V_{K_x}^{J_x,I_x}$ on the condition that their $V(A_{j=J_y}^{i=I_y,q}) = V_{K_y}^{J_y,I_y}$ as:

$$Pr\{V_{K_x}^{J_x,I_x} | V_{K_y}^{J_y,I_y}\} = \frac{||\mathbb{C}(I_x, J_x, K_x) \bigcap \mathbb{C}(I_y, J_y, K_y)||}{||\mathbb{C}(I_y, J_y, K_y)||}, \tag{4}$$

where $||\mathbb{C}(I_x, J_x, K_x) \bigcap \mathbb{C}(I_y, J_y, K_y)||$ is the size of the intersection set of sets $\mathbb{C}(I_x, J_x, K_x)$ and $\mathbb{C}(I_y, J_y, K_y)$ and $||\mathbb{C}(I_y, J_y, K_y)||$ is the size of set $\mathbb{C}(I_y, J_y, K_y)$.

**Proposition 2.** *Given $I_y$, $J_y$ and $K_y$, the set of conditional probabilities $Pr\{V_k^{J_x,I_x} | V_{K_y}^{J_y,I_y}\}$ for $\forall I_x, J_x$ satisfies* $\sum_{V_k^{J_x,I_x} \in \mathbb{V}_{J_x}^{I_x}} Pr\{V_k^{J_x,I_x} | V_{K_y}^{J_y,I_y}\} = 1$.

The proof of Proposition 2 is detailed in Appendix 1.1. As can be seen, $Pr\{V_k^{J_x,I_x} | V_{K_y}^{J_y,I_y}\}, V_k^{J_x,I_x} \in \mathbb{V}_{J_x}^{I_x}$ form a probability distribution in the sample space $\mathbb{V}_{J_x}^{I_x}$. As a result, we formalize the attribute dependency as the probability distribution of values in one attribute $A_{J_x}^{I_x}$ given another attribute's value $V_{K_y}^{J_y,I_y}$:

$$D(A_{J_x}^{I_x} | V_{K_y}^{J_y,I_y}) = \{Pr\{V_k^{J_x,I_x} | V_{K_y}^{J_y,I_y}\}, \forall V_k^{J_x,I_x} \in \mathbb{V}_{J_x}^{I_x}\}, \tag{5}$$

where, $I_x \neq I_y$ or $J_x \neq J_y$. If $I_x \neq I_y$, $D(A_{J_x}^{I_x} | V_{K_y}^{J_y,I_y})$ is a certification path attribute dependency. If $J_x \neq J_y$, but $I_x = I_y$, $D(A_{J_x}^{I_x} | V_{K_y}^{J_y,I_y})$ is a certificate attribute dependency. As the compromised CAs can simply duplicate attributes from the corresponding legitimate sample to the fake certificate, the detection based on certificate attribute dependencies can be evaded. Moreover, the detection relying on $D(A_{J_x}^{I_x} | V_{K_y}^{J_y,I_y}), I_x > 1, I_y > 1, I_x \neq I_y$ can also be circumvented easily because the compromised CAs are capable of issuing intermediate CAs arbitrarily. The reasons have been detailed in Section 3. As a result, SSLight only employs $D(A_{J_x}^{I_x} | V_{K_y}^{J_y,I_y}), I_x = 1, I_y > 1$ to perform its detection.

### *4.2. SSLight Design*

#### 4.2.1. Detection Algorithm

SSLight examines certificates based on a feature set, denoted as $\mathbb{F}$, which includes a sequence of attribute dependencies:

$$\begin{gathered}\mathbb{F} = \{D(A^1_{J_x}|V^{J_y,I_y}_{K_y})\},\ where,\ 1 < I_y \leq N_{max},\\ A^1_{J_x} \in \mathbb{A}^1, A^{I_y}_{J_y} \in \mathbb{A}^{I_y}, V^{J_y,I_y}_{K_y} \in \mathbb{V}^{I_y}_{J_y}.\end{gathered} \tag{6}$$

Let $C^1_e$, where $C^1_e \in \mathbb{C}$ or $C^1_e \notin \mathbb{C}$, be a certificate under examination. If $\exists Pr\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} \in D(A^1_{J_x}|V(A^{I_y,e}_{J_y})) \in \mathbb{F}$ can be considered as a relatively small probability, SSLight regards $C^1_e$ as a fake certificate issued by $C^{I_y>1}_e \in \mathbb{C}$, which is a trusted CA that may be compromised. According to Proposition 3, even if $C^1_e \notin \mathbb{C}$, we may have $C^{I_y>1}_e \in \Gamma(C^1_q) \in \mathbb{C}$. Note that browsers are assumed to not trust $C^{I_y>1}_e \notin \mathbb{C}$ in this paper.

However, the same value of $Pr\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\}$ in different $\mathbb{V}^1_{J_x}$ represents different magnitudes, because $||\mathbb{V}^1_{J_x}||$ (*i.e.*, the sizes of $\mathbb{V}^1_{J_x}$) are different. For example, given $Pr\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} = 0.01$, if $||\mathbb{V}^1_{J_x}|| = 10,000$, this probability can be considered as large compared with $\frac{1}{||\mathbb{V}^1_{J_x}||} = 0.0001$. However, if $||\mathbb{V}^1_{J_x}|| = 2$, the probability $0.01$ is very small in comparison to $\frac{1}{||\mathbb{V}^1_{J_x}||} = 0.5$.

To achieve a fair comparison among different $\mathbb{V}^1_{J_x}$, SSLight introduces a concept of *relative probability*, denoted as $P\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\}$, which can be calculated as:

$$P\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} = Pr\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} \times ||\mathbb{V}^1_{J_x}||. \tag{7}$$

As a result, the probabilities from different $\mathbb{V}^1_{J_x}$ can be equivalently compared in the form of relative probability. Back to the example $Pr\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} = 0.01$, as we have $P\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} = 100$ when $||\mathbb{V}^1_{J_x}|| = 10,000$ and $P\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} = 0.02$ when $||\mathbb{V}^1_{J_x}|| = 2$, this probability can be considered as relatively large when $||\mathbb{V}^1_{J_x}|| = 10,000$, but relatively small in the case $||\mathbb{V}^1_{J_x}|| = 2$.

With the help of the relative probability, SSLight is implemented in Algorithm 1. In this detection algorithm, $P_{th} \geq 0$ is a relative probability threshold, and $||\mathbb{P}^-_{th}||$ represents the number of probabilities whose relative probabilities are no larger than $P_{th}$. If $\exists Pr\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} \in D(A^1_{J_x}|V(A^{I_y,e}_{J_y})) \in \mathbb{F}$, $P\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} \leq P_{th}$ (*i.e.*, $||\mathbb{P}^-_{th}|| > 0$), $C^1_e$ can be regarded as a fake certificate issued from $C^{I_y>1}_e$. Otherwise, $C^1_e$ is a legitimate one.

#### 4.2.2. Attack Range Reduction

Assume $C^{I_y>1}_e$ is compromised and can be used to issue fake certificate $C^1_e$. When SSLight is disabled, $C^{I_y>1}_e$ can assign any possible values to any attributes in $C^1_e$ without causing $C^1_e$ to be detected, such that, for $\forall A^1_{J_x} \in \mathbb{A}^1$, $V(A^{1,e}_{J_x}) = V^{J_x,1}_k, \forall V^{J_x,1}_k \in \mathbb{V}^1_{J_x}$. As a result, there are $\prod_{A^1_{J_x} \in \mathbb{A}^1} ||\mathbb{V}^1_{J_x}||$ possible value combinations that $C^{I_y>1}_e$ can assign to $C^1_e$'s attributes. The number of possible value combinations, $\prod_{A^1_{J_x} \in \mathbb{A}^1} ||\mathbb{V}^1_{J_x}||$, is defined as $C^{I_y>1}_e$'s attack range, which reflects $C^{I_y>1}_e$'s capability for issuing fake certificates. SSLight can help limit $C^{I_y>1}_e$'s attack range, because a number of values in attribute $A^{1,e}_{J_x}$ may cause $P\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} \leq P_{th}$, thus making them unable to be assigned.

**Algorithm 1:** Whether $C_e^1$ is a fake certificate from $C_e^{I_y>1}$.

**Input**: $C_e^1$ and $C_e^{I_y>1}$

$||\mathbb{P}_{th}^-|| \leftarrow 0$;
**for all** $J_x, J_y$, in $D(A_{J_x}^1|V(A_{J_y}^{I_y,e})) \in \mathbb{F}$ **do**
  **if** $P\{V(A_{J_x}^{1,e})|V(A_{J_y}^{I_y,e})\} \leq P_{th}$ **then**
    $||\mathbb{P}_{th}^-|| \leftarrow ||\mathbb{P}_{th}^-|| + 1$;
  **end if**
**end for**
**if** $||\mathbb{P}_{th}^-|| > 0$ **then**
  **return** $C_e^1$ is a fake certificate issued by $C_e^{I_y>1}$;
**else**
  **return** $C_e^1$ is a legitimate one issued by $C_e^{I_y>1}$;
**end if**

In the case that if SSLight employs only one attribute dependency $D(A_{J_x}^1|V(A_{J_y}^{I_y,e})) \in \mathbb{F}$ to detect fake certificates issued from $C_e^{I_y>1}$, $\mathbb{V}_{J_x}^1$ can be divided into two subsets as $\mathbb{V}_{J_x}^1 = \mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e}) + \mathbb{V}_{J_x}^{1-}(P_{th}, A_{J_y}^{I_y,e})$, where:

$$\begin{aligned}\mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e}) &= \{\forall V_k^{J_x,1} \in \mathbb{V}_{J_x}^1, P\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} > P_{th}\},\\ \mathbb{V}_{J_x}^{1-}(P_{th}, A_{J_y}^{I_y,e}) &= \{\forall V_k^{J_x,1} \in \mathbb{V}_{J_x}^1, P\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} \leq P_{th}\}.\end{aligned} \tag{8}$$

As a result, the single attribute dependency $D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$ can help reduce $C_e^{I_y>1}$'s attack range, which is restricted to $A_{J_x}^1$ and specified by $V(A_{J_y}^{I_y,e})$, from $||\mathbb{V}_{J_x}^1||$ to $||\mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e})||$. We define an attack range reduction factor, $R(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$, to represent this kind of attack range reduction as:

$$R(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = \frac{||\mathbb{V}_{J_x}^1||}{||\mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e})||}, \tag{9}$$

A larger $R(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$ leads to a better detection capability obtained by the attribute dependency $D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$. Corollary 1, which is proven in Appendix 1.9, shows the upper bound and lower bound of $R(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$.

**Corollary 1.** *The attack range reduction factor satisfies* $1 \leq R(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \leq \infty$. *In particular,* $1 \leq R(P_{th} < 1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \leq ||\mathbb{V}_{J_x}^1||$.

When considering all of the attribute dependencies in $\mathbb{F}$, SSLight abates $C_e^{I_y>1}$'s attack range from $\prod_{A_{J_x}^1 \in \mathbb{A}^1} ||\mathbb{V}_{J_x}^1||$ to $\prod_{A_{J_x}^1 \in \mathbb{A}^1} ||\bigcap_{A_{J_y}^{I_y} \in \mathbb{A}^{I_y}} \mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e})||$. We thus use an attack range reduction power, $R^*(P_{th}, C_e^{I_y>1})$, to measure the detection capability obtained by SSLight as:

$$R^*(P_{th}, C_e^{I_y>1}) = \prod_{A_{J_x}^1 \in \mathbb{A}^1} \frac{||\mathbb{V}_{J_x}^1||}{||\bigcap\limits_{A_{J_y}^{I_y} \in \mathbb{A}^{I_y}} \mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e})||}. \tag{10}$$

Based on Equation (10), we have Corollaries 2 and 3, which are proven in Appendixes 1.10 and 1.11, respectively.

**Corollary 2.** *The attack range reduction power satisfies* $1 \leq R^*(P_{th}, C_e^{I_y>1}) \leq \infty$. *In particular,* $1 \leq R^*(P_{th}=0, C_e^{I_y>1}) \leq \prod_{A_{J_x}^1 \in \mathbb{A}^1} ||\mathbb{V}_{J_x}^1||$.

**Corollary 3.** *Even if* $\forall A_{J_x}^1 \in \mathbb{A}^1, \forall A_{J_y}^{I_y} \in \mathbb{A}^{I_y}, R(P_{th}>0, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \neq \infty$, *we may still have* $R^*(P_{th}>0, C_e^{I_y>1}) = \infty$.

4.2.3. False Positive

According to Equations (8) and (9), a single attribute dependency $D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$ can achieve a larger reduction factor with a larger $P_{th}$. However, this larger $P_{th}$ consequently causes a larger false positive, which is the ratio of legitimate certificates that are wrongly regarded as fake certificates in the legitimate sample set $\mathbb{C}$. The false positive with respect to the single attribute dependency $D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$ can be calculated as:

$$E(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = \sum_{V_k^{J_x,1} \in \mathbb{V}_{J_x}^{1-}(P_{th}, A_{J_y}^{I_y,e})} Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\}. \tag{11}$$

where $0 \leq E(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \leq 1$. As defined in Equation (8), $\forall V_k^{J_x,1} \in \mathbb{V}_{J_x}^{1-}(P_{th}, A_{J_y}^{I_y,e})$ will cause SSLight with the single attribute dependency $D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$ to regard the examined certificate as a fake one; thus, their corresponding probabilities contribute to the false positive. As a larger $P_{th}$ leads to a larger $||\mathbb{V}_{J_x}^{1-}(P_{th}, A_{J_y}^{I_y,e})||$, the false positive $E(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$ can be increased when $P_{th}$ grows.

For SSLight with feature set $\mathbb{F}$, its false positive caused by $C_e^{I_y>1}$ can be computed as follows.

$$\begin{aligned} E^*(P_{th}, C_e^{I_y>1}) &= \frac{||\bigcap_{A_{J_y}^{I_y} \in \mathbb{A}^{I_y}} \bigcup_{A_{J_x}^1 \in \mathbb{A}^1} (\mathbb{C}_{J_x}^- \bigcap \mathbb{C}(I_y, J_y, k'))||}{||\bigcap_{A_{J_y}^{I_y} \in \mathbb{A}^{I_y}} \mathbb{C}(I_y, J_y, k')||}, \\ where\ V(A_{J_y}^{I_y,e}) &= V_{k'}^{J_x,I_x},\ \mathbb{C}_{J_x}^- = \bigcup_{V_k^{J_x,1} \in \mathbb{V}_{J_x}^{1-}(P_{th}, A_{J_y}^{I_y,e})} \mathbb{C}(1, J_x, k). \end{aligned} \tag{12}$$

$\mathbb{C}_{J_x}^-$ includes the legitimate samples, which are falsely regarded as fake in $\mathbb{C}$ when the $D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$ is used for the detection. The operator $\bigcup_{A_{J_x}^1 \in \mathbb{A}^1}$ is used to unify the samples that are wrongly detected, and the operator $\bigcap_{A_{J_y}^{I_y} \in \mathbb{A}^{I_y}}$ helps select samples that are issued from $C_e^{I_y>1}$. Note that both of the two false positive definitions, Equations (11) and (12), have not taken legitimate certificates outside the legitimate sample set $\mathbb{C}$, $C_e^1 \notin \mathbb{C}$, into consideration.

According to Equations (8)–(12), we conclude Corollaries 4–6, which can guide SSLight to choose appropriate $P_{th}$ to balance attack range reduction and false positives. Their proofs are detailed in Appendixes 1.7–1.12.

**Corollary 4.** *When* $P_{th} = 0$, *for* $\forall D(A_{J_x}^1|V(A_{J_y}^{I_y,e})) \in \mathbb{F}$, $E(0, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = 0$ *and* $E^*(0, C_e^{I_y>1}) = 0$.

**Corollary 5.** $R(P_{th} \geq 1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = \infty \Leftrightarrow E(P_{th} \geq 1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = 1$.

**Corollary 6.** $R^*(P_{th} \geq 1, C_e^{I_y>1}) = \infty \Rightarrow E^*(P_{th} \geq 1, C_e^{I_y>1}) = 1$ *but* $E^*(P_{th} \geq 1, C_e^{I_y>1}) = 1 \not\Rightarrow R^*(P_{th} \geq 1, C_e^{I_y>1}) = \infty$.

### *4.3. Theoretical Analysis*

According to Equation (5), we calculate attribute dependencies between attributes as conditional probability distributions based on a training set of legitimate certificates. As a result, SSLight's detection capability, in terms of the attack range reduction and false positives, mainly depends on the prior distributions among legitimate samples in the training set. For example, assuming $C_e^{I_y>1}$ is a compromised CA, when SSLight employs $P_{th} = 1$ and $D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$ with $||\mathbb{V}_{J_x}^1|| = 2$ to perform the detection, the case that $Pr\{V_1^{J_x,1}|V(A_{J_y}^{I_y,e})\} = 1$ and $Pr\{V_2^{J_x,1}|V(A_{J_y}^{I_y,e})\} = 0$ consequently results in $R(1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = 2$ and $E(1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = 0$. However, if the prior distribution is $Pr\{V_1^{J_x,1}|V(A_{J_y}^{I_y,e})\} = Pr\{V_2^{J_x,1}|V(A_{J_y}^{I_y,e})\} = 0.5$, the reduction factor $R(1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = \infty$ with the false positive $E(1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = 1$ is achieved.

To assess the impacts on the detection capability caused by the corresponding prior distribution in each attribute dependency $D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$, we propose an evaluation function.

We propose to use a metric, $\phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$, to quantify the impacts on the detection capability and false positives caused by the legitimate distribution. Given $P_{th}$ and $\mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$, for the compromised CA $C_e^{I_y>1}$, $\phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$ can be computed as:

$$\phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = \sum_{V_k^{J_x} \in \mathbb{V}_{J_x}} |Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} - \tfrac{P_{th}}{||\mathbb{V}_{J_x}||}|. \tag{13}$$

where $|Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} - \frac{P_{th}}{||\mathbb{V}_{J_x}||}|$ is the absolute value of $Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} - \frac{P_{th}}{||\mathbb{V}_{J_x}||}$.

**Proposition 3.** *The metrics* $\phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$ *represent the underlying detection capability and false positives, as:*

$$\phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = -2 \times E(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) - \frac{2 \times P_{th}}{R(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e})))} + 1 + P_{th}.$$

According to Proposition 3, a better detection capability and a lower false positive cause a larger metric $\phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$. Thus, the metric is able to guide SSLight's feature selection. The attribute dependencies with larger $\phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$ receive a higher priority to be chosen. Based on Proposition 3, we have three corollaries as follows.

**Corollary 7.** *The metric* $\phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e})))$ *satisfies* $0 \leq \phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \leq 1 + P_{th} - \frac{2 \times P_{th}}{||\mathbb{V}_{J_x}||}$.

**Corollary 8.** *When* $P_{th} = 0$, $E^{\mathbb{F}}(P_{th}, C_e^{I_y>1}) \equiv 0$ *and* $\forall \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e})) \in \mathbb{F}$, $E(0, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \equiv 0$.

**Corollary 9.** *When* $P_{th} = 1$, *the metric satisfies* $0 \leq \phi(1, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \leq \frac{2 \times (||\mathbb{V}_{J_x}|| - 1)}{||\mathbb{V}_{J_x}||}$. *In particular, the lower bound zero is obtained if* $\mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e}))$ *follows the uniform distribution. Additionally, the upper bound* $\frac{2 \times (||\mathbb{V}_{J_x}|| - 1)}{||\mathbb{V}_{J_x}||}$ *is received if a certain value of* $A_{J_x}^1$ *occupies the probability one.*

Corollary 7 gives the theoretical upper bound and lower bound of the metrics. $\phi(P_{th}, \mathbb{D}(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = 0$ indicates that the legitimate distribution of attribute dependency

$\mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))$ is inadequate to perform the detection when the threshold is $P_{th}$. $\phi(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) = 1 - P_{th} - \frac{2\times P_{th}}{||\mathbb{V}_{J_x}||}$, on the other hand, represents that the legitimate distribution can achieve the best detection capability with the lowest false positive when the threshold is $P_{th}$. In particular, Corollary 8 elaborates on the special case for $P_{th} = 0$, in which the false positive identically equals zero for any distributions of the attribute dependency. However, in this case, we have $\phi(0, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) \equiv 1$, as well; the metric thus loses the functionality to measure the detection capability in terms of the attack range reduction factor. As the false positive is fixed at zero, we can use $R(0, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$ instead of $\phi(0, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$ to guide the feature selection if $P_{th} = 0$.

Corollary 9 instantiates the metric's upper bound and lower bound when $P_{th} = 1$, which allows SSLight to regard $C^1_e$ as a fake one if $\exists Pr\{V(A^{1,e}_{J_x})|V(A^{I_y,e}_{J_y})\} \leq \frac{1}{||\mathbb{V}_{J_x}||}$. $\frac{1}{||\mathbb{V}_{J_x}||}$ is the probability representing the uniform distribution. In this case, the attribute dependency with a uniform distribution is not suitable for the detection, because it causes the highest false positive, $E(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) = 1$. By contrast, if a certain value of $A^1_{J_x}$ receives the probability one in an attribute dependency $\mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))$, the best detection capability, $R(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) = ||\mathbb{V}_{J_x}||$, and the lowest false positive, $E(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) = 0$, are both achieved.

The proof of Proposition 3 and Corollaries 7–9 are detailed in Appendixes 1.9–1.12, respectively.

## 5. Evaluation

In this section, we first explain the experiment setup, which includes the legitimate sample set and feature set used in SSLight. Based on that, we evaluate each single attribute dependency's detection capability in terms of its attack range reduction factor and false positive in different $P_{th}$. SSLight thus selects appropriate attribute dependencies in accordance with the feature evaluation results to achieve a large attack range reduction power with a low false positive. SSLight is consequently implemented as a Firefox add-on and used to expose real-world fake certificates with a $100\%$ accuracy.

### *5.1. Experiment Setup*

The SSL Observatory project [6] has conducted a thorough scan on all allocated IPv4 space in the default port of HTTPS (*i.e.*, 443) and receives $1,455,391$ valid certificates in its dataset [22]. We further select the web server certificates whose attribute *CA* is *FALSE* and trace their corresponding certification paths. Finally, we obtain $830,306$ such samples, which have been employed by SSLight as the legitimate sample set $\mathbb{C}$ in this paper. In this set, the depth of the longest certification path is limited to 5 (*i.e.*, $I_y \leq N_{max} = 5$) because we observe that less than $4\%$ of certification paths are longer than 5 in legitimate samples. More precisely, we have $100\%$, $83.2\%$, $67.3\%$ and $3.02\%$ of the $830,306$ samples whose $I_y = 2, 3, 4$ and 5, respectively.

According to RFC5280 [2] and X.520 [17], X.509 certificates have more than 120 attribute definitions, which includes around 60 *Subject* attributes. However, many of these attributes may not be appropriate in the design of SSLight, because they cannot provide useful information for the detection. An example is the attribute *CA*. $\forall C^1_e$ have *CA*=*FALSE*, and $\forall C^{I_y>1}_e$ have *CA*=*TRUE*. As a result, the attribute *CA* has a deterministic, but undistinguished, value in both legitimate and fake certificates. As another example, the value of attribute *Signature* is unique in different certificates and will be changed even when the

certificate is updated. Thus, this attribute loses its functionality to provide information to distinguish the legitimate and fake certificates. As shown in Table 1, we choose 8 appropriate attributes in $\mathbb{A}^1$ and $\mathbb{A}^{I_y>1}$, respectively. For any $C_e^{I_y>1}$, we thus have 64 attribute dependencies $D(A^1_{J_x}|V(A^{I_y,e}_{J_y})) \in \mathbb{F}$ in SSLight. For $\forall A^1_{J_x} \in \mathbb{A}^1$, $||\mathbb{V}^1_{J_x}||$ is the size of $A^1_{J_x}$'s value set. In this paper, we calculate $||\mathbb{V}^1_{J_x}||$ as the number of distinct values appearing in $A^1_{J_x}$ among $\mathbb{C}$. $||\mathbb{V}^1_{J_x}||$'s calculation includes the value *Empty*.

**Table 1.** Considered attributes $A^1_{J_x} \in \mathbb{A}^1$ and $A^{I_y>1}_{J_y} \in \mathbb{A}^{I_y>1}$.

| $A^1_{J_x}$ | $A^{I_y>1}_{J_y}$ | Name | Abbreviation | $\|\|\mathbb{V}^1_{J_x}\|\|$ |
|---|---|---|---|---|
| N/A | $A^{I_y>1}_1$ | CommonName | CN | N/A |
| $A^1_1$ | $A^{I_y>1}_2$ | Country | C | 211 |
| $A^1_2$ | $A^{I_y>1}_3$ | Description | DC | 8 |
| $A^1_3$ | $A^{I_y>1}_4$ | Locality | L | 27,947 |
| $A^1_4$ | $A^{I_y>1}_5$ | StateOrProvince | ST | 7020 |
| $A^1_5$ | $A^{I_y>1}_6$ | Organization | O | 628,401 |
| $A^1_6$ | $A^{I_y>1}_7$ | OrganizationUnit | OU | 38,606 |
| $A^1_7$ | $A^{I_y>1}_8$ | PublicKeyAlgorithm | N/A | 2 |
| $A^1_8$ | N/A | KeyLength | N/A | 57 |

### *5.2. Feature Evaluation*

In order to evaluate the detection capability for each $D(A^1_{J_x}|V(A^{I_y,e}_{J_y})) \in \mathbb{F}$, we conduct extensive analysis for their attack range reduction factor $R(P_{th}, D(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$ and the corresponding false positive $E(P_{th}, D(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$ when $P_{th} = 0$ and $P_{th} = 1$, respectively. According to Corollary 1, when $P_{th} = 0 < 1$, the attack range reduction factor satisfies $1 \leq R(0, D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) \leq ||\mathbb{V}^1_{J_x}||$. In this case, $D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))$ has different reduction factor upper bounds for different $A^1_{J_x}$. Figure 4a–h illustrates $R(P_{th}, D(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$'s CDF plots for different $I_y > 1$. It can be seen that the attack range specified by $V(A^{I_y>1,e}_{J_y})$ in a smaller $I_y$ always receives a larger reduction. For $\forall D(A^1_{J_x}|V(A^{I_y,e}_{J_y})) \in \mathbb{F}$, at least 30% of $V(A^{I_y=2,e}_{J_y})$s' attack range is reduced to 1, which indicates the upper bound of reduction factor $R(0, D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) = ||\mathbb{V}^1_{J_x}||$. However, only less than 10% of $V(A^{I_y=5,e}_{J_y})$s' attack range can be decreased to 1. Particularly, this percentage is further dropped to 0% when $A^{I_x=1}_5$=*Organization* and $A^{I_x=1}_6$=*OrganizationUnit*. In Figure 4i, we also show the average reduction factor over all of the available attributes in the certificates that we have in our dataset. All of these results demonstrate that the single attribute dependency has a better capability to detect false certificates issued from $C_e^{I_y>1}$ with a smaller $I_y$.

When the $P_{th}$ is increased from 0 to 0.5 and eventually to 1, the reduction factor will be increased at the sacrifice of enlarging false positives. As can be seen in Figure 5a–i, all of the $R(P_{th} = 1, D(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$ for $\forall D(A^1_{J_x}|V(A^{I_y,e}_{J_y})) \in \mathbb{F}$ are no smaller than $R(P_{th} = 0, D(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$. Figure 6a–i, on the other hand, demonstrates that the corresponding false

positives in $P_{th} = 1$ are no smaller than that in $P_{th} = 0$. In accordance with Corollary 4, the false positive remains 0 when $P_{th} = 0$ (*i.e.*, $E(P_{th} = 0, D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) = 0$) in our experiments. When $P_{th} = 1$ and $A^{I_x=1}_5 \neq$*Organization*, all of the false positives are less than 0.2. These small false positives help increase the reduction factors in $P_{th} = 1$ to a little bit larger than that in $P_{th} = 0$. The case $A^{I_x=1}_5 =$*Organization* with $P_{th} = 1$ introduces 4 false positives larger than 0.7, but the corresponding reduction factor shows nearly no increase in Figure 5e. Note that, although $R(P_{th} = 1, D(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$ can reach $\infty$, as explained in Corollary 1, we have not observed $\infty$ when $P_{th} = 1$ in our experiments. Moreover, we show the reduction factor and false positive for the results over all available attributes in the certificates in Figures 5i and 6i. As can be seen, more than a 50% reduction factor is larger than $10^4$, and less than 5% suffers from a false positive larger than 0.1. It is worth noting that, when we apply SSLight to real-world scenarios, any one abnormal attribute dependency can expose the fake certificates. As a result, the actual detection capability is much better than that we show through the mean value.

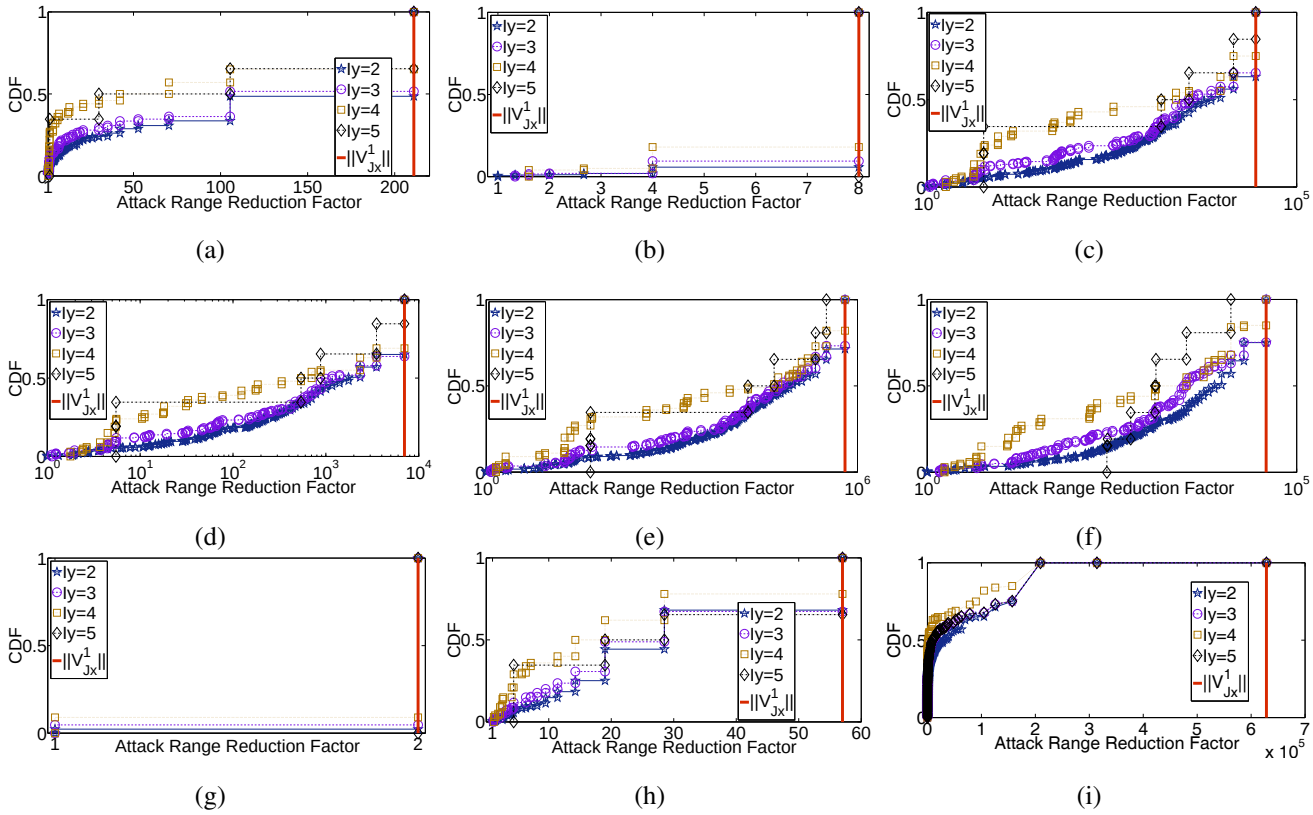



**Figure 4.** Attack range reduction factor for different $D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))$ when $P_{th} = 0$ and $C^{I_y>1}_e$ in different $I_y$. (**a**) $A^1_1$ = *Country*; (**b**) $A^1_2$ = *Description*; (**c**) $A^1_3$ = *Locality*; (**d**) $A^1_4$ = *StateOrProvince*; (**e**) $A^1_5$ = *Organization*; (**f**) $A^1_6$ = *OrganizationUnit*; (**g**) $A^1_7$ = *PublicKeyAlgorithm*; (**h**) $A^1_8$ = *KeyLength*; (**i**) average result over all available attributes.

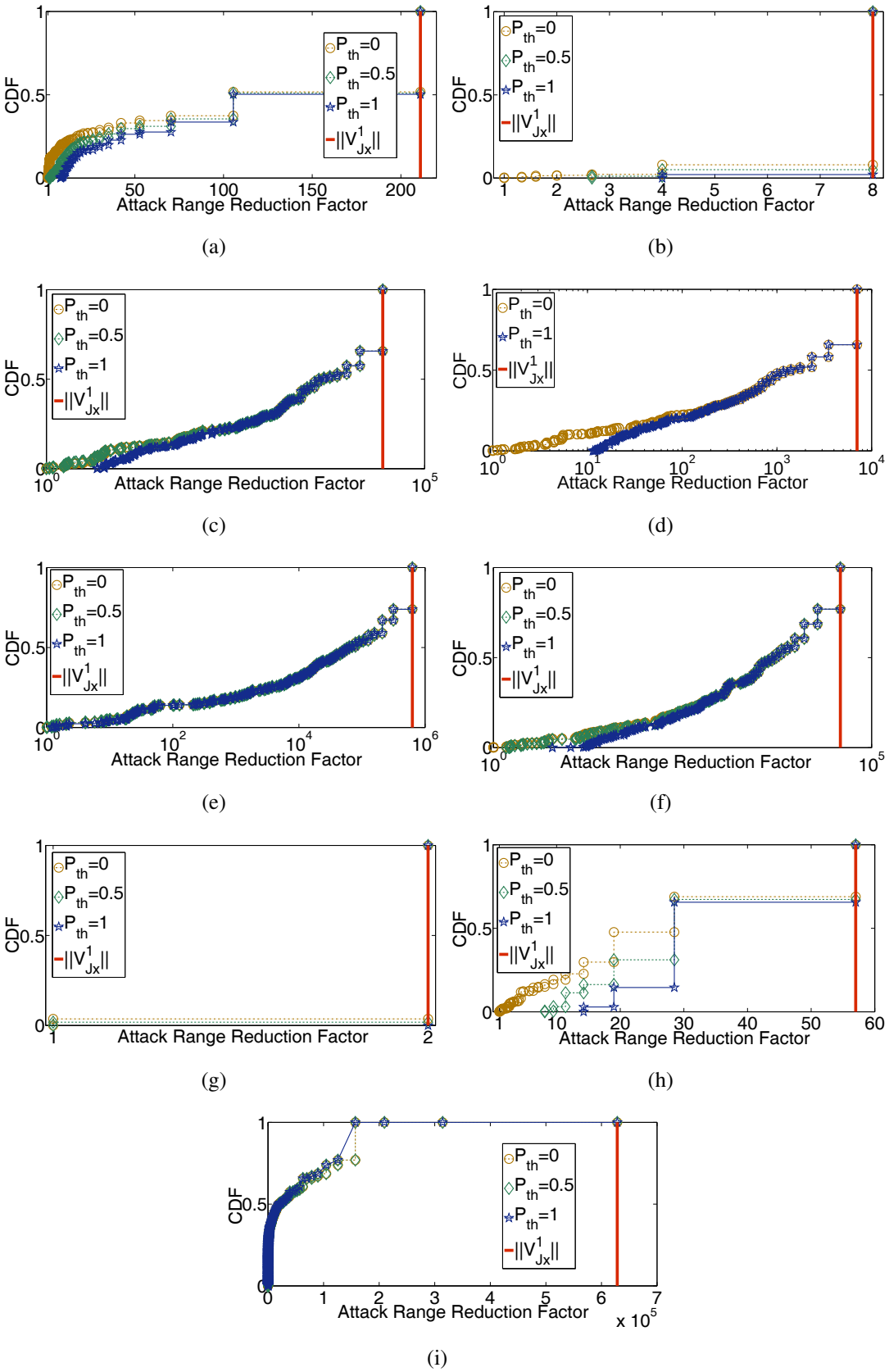



**Figure 5.** Attack range reduction factor for different $D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))$ when $P_{th} = 0$, $P_{th} = 0.5$ and $P_{th} = 1$. (**a**) $A^1_1$ = *Country*; (**b**) $A^1_2$ = *Description*; (**c**) $A^1_3$ = *Locality*; (**d**) $A^1_4$ = *StateOrProvince*; (**e**) $A^1_5$ = *Organization*; (**f**) $A^1_6$ = *OrganizationUnit*; (**g**) $A^1_7$ = *PublicKeyAlgorithm*; (**h**) $A^1_8$ = *KeyLength*; (**i**) average result over all available attributes.

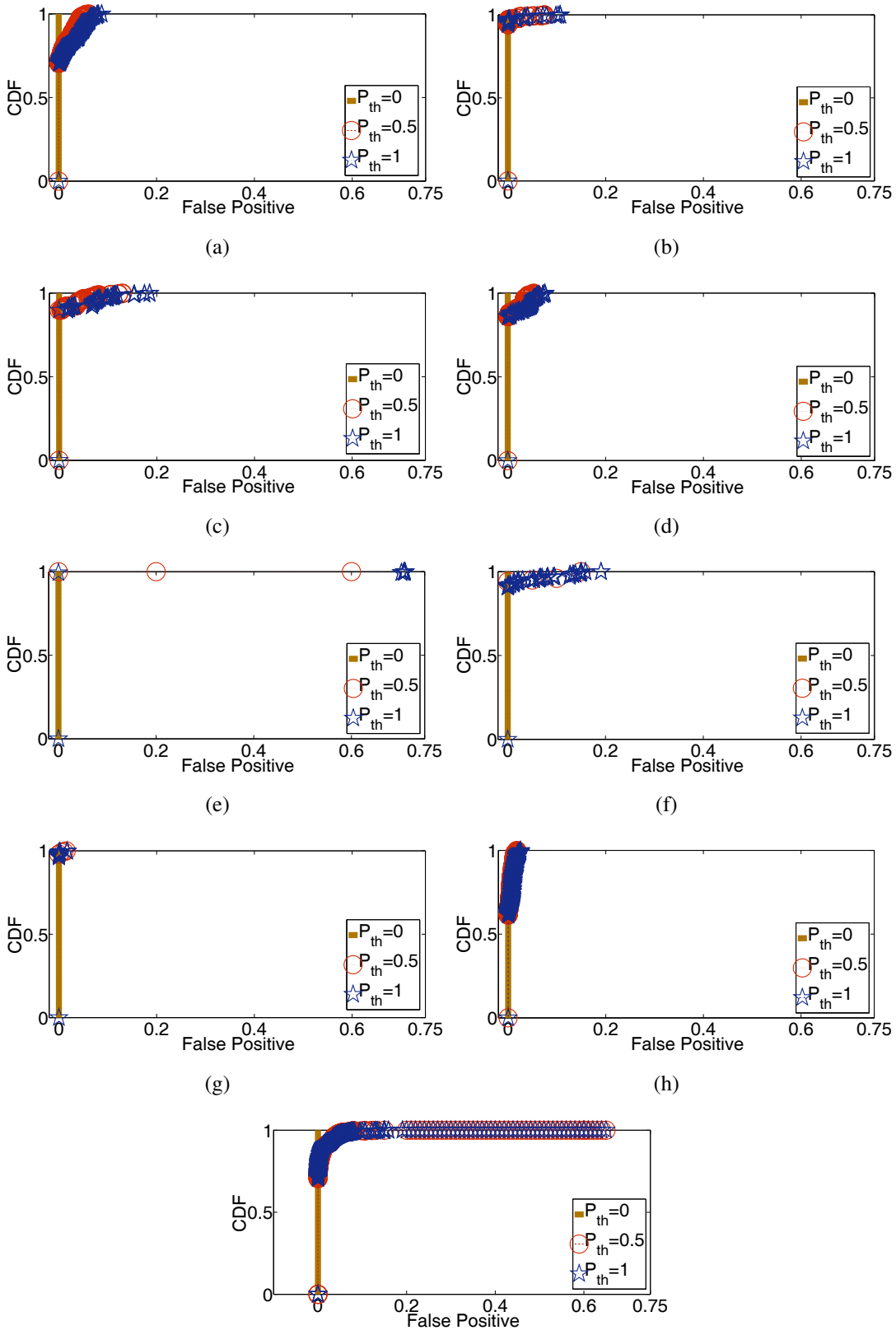
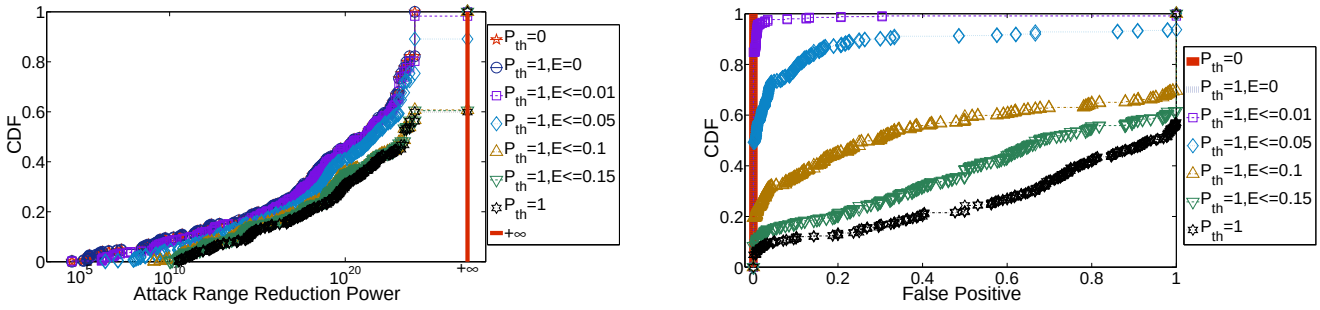



**Figure 6.** False positives for different $D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))$ when $P_{th} = 0$, $P_{th} = 0.5$ and $P_{th} = 1$. (**a**) $A^1_1$ = *Country*; (**b**) $A^1_2$ = *Description*; (**c**) $A^1_3$ = *Locality*; (**d**) $A^1_4$ = *StateOrProvince*; (**e**) $A^1_5$ = *Organization*; (**f**) $A^1_6$ = *OrganizationUnit*; (**g**) $A^1_7$ = *PublicKeyAlgorithm*; (**h**) $A^1_8$ = *KeyLength*; (**i**) average result over all available attributes.

### *5.3. SSLight Evaluation*

When SSLight employs $\forall D(A^1_{J_x}|V(A^{I_y,e}_{J_y})) \in \mathbb{F}$ for the detection, the attack range reduction power $R^*(P_{th}, C_e^{I_y>1})$ and false positive $E^*(P_{th}, C_e^{I_y>1})$ can be used to measure its capability for exposing false certificates issued from $C_e^{I_y>1}$. Figure 7a,b shows the CDF of $R^*(P_{th}, C_e^{I_y>1})$ and $E^*(P_{th}, C_e^{I_y>1})$, respectively. When $P_{th} = 1$, SSLight obtains more than $40\%$ of $R^*(P_{th} = 1, C_e^{I_y>1}) = \infty$, in which $\infty$ is the upper bound of $R^*(P_{th}, C_e^{I_y>1})$ when $P_{th} > 0$, according to Corollaries 2 and 3. When $P_{th} = 0$, no more than $20\%$ of $R^*(P_{th} = 0, C_e^{I_y>1})$ reaches $\prod_{A^1_{J_x} \in \mathbb{A}^1} ||\mathbb{V}^1_{J_x}|| \approx 8.2 \times 10^{23}$, the upper bound of the reduction power when $P_{th} = 0$. In accordance with Corollary 4, the false positive $E^*(P_{th} = 0, C_e^{I_y>1})$ remains $0$. Moreover, we observe that at least $\prod_{A^1_{J_x} \in \mathbb{A}^1} ||\mathbb{V}^1_{J_x}|| - \frac{\prod_{A^1_{J_x} \in \mathbb{A}^1} ||\mathbb{V}^1_{J_x}||}{R^*(P_{th}=0, C_e^{I_y>1})} = 8.2 \times (10^{23} - 10^{18})$ fake certificates issued from $C_e^{I_y>1}$ can be detected. As a result, SSLight is shown to be able to expose the vast majority of fake certificates issued from trusted, but compromised CAs with $0$ false positives.




(a) (b)

**Figure 7.** Reduction power and false positive when $P_{th} = 0$ and $P_{th} = 1$ with different feature exclusion in SSLight. (**a**) Attack range reduction power in SSLight; (**b**) false positive in SSLight.

Although $R^*(P_{th} = 1, C_e^{I_y>1})$ obtains at least $10^5$ times larger than $R^*(P_{th} = 0, C_e^{I_y>1})$, more than $42\%$ of false positives $E^*(P_{th} = 1, C_e^{I_y>1}) = 1$. $E^*(P_{th}, C_e^{I_y>1}) = 1$ is not acceptable, because SSLight will wrongly regard $\forall C^1_q \in \mathbb{C}$ as fake certificates. However, as shown in Figure 6, more than $95\%$ $E(P_{th} = 1, D(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$ is $0$. We thus observe that the combination of a small number of features with small positives may cause a large positive in SSLight. To mitigate this impact, SSLight uses a false positive threshold to filter some of the features whose $E(P_{th} = 1, D(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$ is larger than that threshold. As shown in Figure 7, when we exclude features when the threshold of $E(P_{th} = 1, D(A^1_{J_x}|V(A^{I_y,e}_{J_y})))$ is decreased from $0.15$ down to $0$, the probability of $E^*(P_{th} = 1, C_e^{I_y>1}) = 1$ is dropped from more than $42\%$ down to $0\%$, as well. In this case, the corresponding $R^*(P_{th} = 1, C_e^{I_y>1})$ is also decreased to the same as $R^*(P_{th} = 0, C_e^{I_y>1})$. This feature exclusion process shows how the single feature's false positive affects SSLight's false positive. Appendix 1.8 lists the excluded features whose $E(P_{th} = 1, D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) > 0.15$.

### *5.4. Firefox Add-On and Real-World Examples*

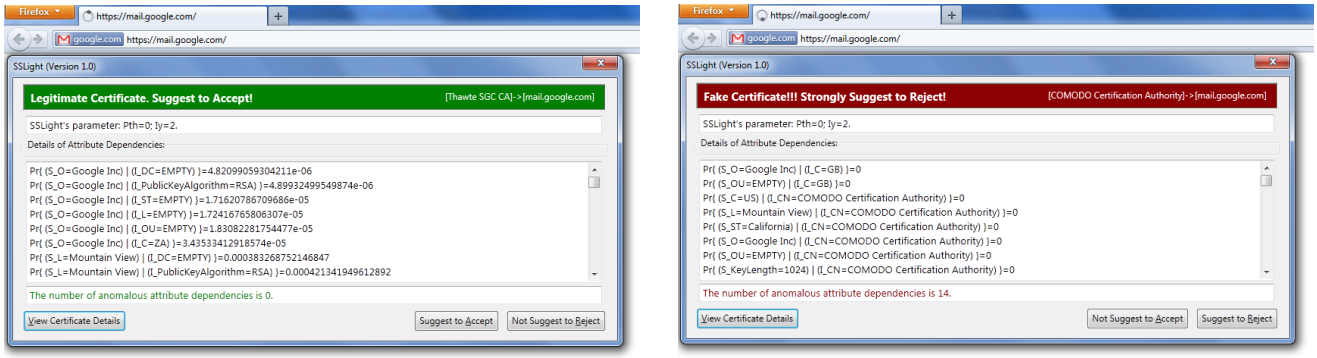
In this paper, SSLight is implemented as a Firefox add-on to help Firefox detect fake certificates issued from the compromised CAs in HTTPS connections. In this implementation, a "http-on-examine-response" event is added to observe all of the HTTP responses, and the interface nsIHttpChannel is used to access the HTTP channels. If nsIHttpChannel.securityInfo indicates STATE_IS_SECURE, the channel is realized as an HTTPS connection. The add-on thus accesses interfaces nsISSLStatusProvider and nsISSLStatus and obtains the X.509 certificate $C_e^1$ in the channel by calling nsISSLStatus.serverCert. Thus, for $\forall A_{J_x}^1 \in \mathbb{A}^1$ and $\forall A_{J_y}^{I_y>1} \in \mathbb{A}^{I_y>1}$, the corresponding $Pr\{V(A_{J_x}^{1,e})|V(A_{J_y}^{I_y,e})\}$ can be queried from an SQLite file, which includes the prior distribution for $\forall D(A_{J_x}^1|V(A_{J_y}^{I_y,e})) \in \mathbb{F}$ calculated using the legitimate sample set presented in Section 5.1. SQLite is a lightweight database that can be used by a Firefox add-on.

As a real-world example, we use the Firefox add-on to examine real-world fake certificates issued from DigiNotar and Comodo. As reported in the Pastebin Blog [23], a DigiNotar CA (*CommonName* = DigiNotar Public CA 2025) has issued a fake certificate to *.google.com. Similarly, Comodo Fraud Incident [24] announces that the Comodo CA has been intruded and issued nine fake certificates across seven different domains, including www/mail.google.com, *.add-ons.mozilla.com, login.live.com, login.yahoo.com, *.skype.com and global trustee. As we cannot obtain the real cases of these fake certificates, we set up two private CAs to impersonate DigiNotar and Comodo, which have been detailed in Section 3. As DigiNotar Public CA 2025 is only an intermediate CA and not trusted by browsers, including Firefox, IE and Chrome, in default, we let our private DigiNotar CA mimic its root CA, DigiNotar Root CA, instead.

We exclude the fake certificate of global trustee in this evaluation because the global trustee does not correspond to a website. As the three fake login.yahoo.com certificates are distinguished as they have different *Serial Number*, which is not an attribute considered by SSLight in this paper, we regard them as the same fake certificate. As a result, we have seven real-world fake certificates for evaluation: one is from DigiNotar, and the other six are issued by Comodo. To extend the real-world evaluation, we just use both DigiNotar and Comodo to issue all seven fake certificates. Moreover, as compromised CAs can arbitrarily issue fake intermediate CAs to change their position in the certification path, DigiNotar and Comodo can stay at $\forall I_y \leq ||\Gamma(C_e^1)||$ to issue $C_e^1$.

In Figure 8, SSLight examines certificates when a user accesses https://mail.google.com in Firefox. In this case, $P_{th}$ is set to zero to mitigate false positives, and only $\forall D(A_{J_x}^1|V(A_{J_y}^{I_y=2,e})) \in \mathbb{F}$ are used. As can be seen in Figure 8a, the legitimate certificate is accepted by SSLight, and the smallest $Pr\{V(A_{J_x}^{1,e})|V(A_{J_y}^{I_y=2,e})\}$ equals $4.82 \times 10^{-6}$, in which $A_{J_x}^{1,e}$ is $A_5^{1,e}$ =*Organization* with the value *Google Inc* and $A_{J_y}^{I_y,e}$ is $A_3^{2,e}$ =*Description* with the value *Empty*. Figure 8b, in contrast, demonstrates that SSLight successfully detects the fake mail.google.com certificate issued from Comodo. $||\mathbb{P}_{th}^-|| = 14 > 0$, indicating that 14 probabilities' relative values are no larger than $P_{th} = 0$, helping SSLight to expose this fake certificate. Table 2 lists the detection results for the seven real-world examples, including their legitimate and fake certificates. As can be seen, SSLight exposes the fake certificates from both DigiNotar and Comodo with 100% accuracy. However, false alarms occur when SSLight examines the legitimate certificates of *.skype.com. The root cause of this false alarm is that some of the legitimate

attribute dependencies do not exist in the sample set. As a result, SSLight is encouraged to use a more comprehensive legitimate sample set to mitigate such an issue. Note that this result does not conflict with Corollary 4, because the legitimate certificate of *.skype.com is not included in our legitimate sample set, $C_7^1 \notin \mathbb{C}$.




(a) (b)

**Figure 8.** SSLight works as a Firefox add-on to examine the legitimate and fake mail.google.com certificates. (**a**) SSLight accepts the legitimate mail.google.com certificate issued by Thawte SGC; (**b**) SSLight rejects the fake mail.google.com certificate issued by Comodo.

**Table 2.** Detection results for 7 discovered fake certificates [23,24] from DigiNotar and Comodo in SSLight with $P_{th} = 0$, $P_{th} = 0.5$ and $P_{th} = 1$ (the three different $P_{th}$ lead to the same result). Domain name (DN): ①, * /www/mail.google.com, ②, * .add-ons.mozilla.com, ③, login.live.com, ④, login.yahoo.com, ⑤, * .skype.com.

| DN | $C_e^1$ | $\|\|\Gamma(C_e^1)\|\|$ | CA | $I_y$ | $\|\|\mathbb{P}_{th}^-\|\|$ | Result | CA | $I_y$ | $\|\|\mathbb{P}_{th}^-\|\|$ | Result | CA | $I_y$ | $\|\|\mathbb{P}_{th}^-\|\|$ | Result |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ① | $C_{1,2,3}^1$ | 3 | Legitimate | 2 | 0 | Legitimate | DigiNotar | 2 | 16 | Fake! | Comodo | 2 | 14 | Fake! |
| | | | | 3 | 0 | Legitimate | | 3 | 18 | Fake! | | 3 | 6 | Fake! |
| ② | $C_4^1$ | 3 | | 2 | 0 | Legitimate | | 2 | 17 | Fake! | | 2 | 13 | Fake! |
| | | | | 3 | 0 | Legitimate | | 3 | 18 | Fake! | | 3 | 5 | Fake! |
| ③ | $C_5^1$ | 3 | | 2 | 0 | Legitimate | | 2 | 18 | Fake! | | 2 | 11 | Fake! |
| | | | | 3 | 0 | Legitimate | | 3 | 19 | Fake! | | 3 | 6 | Fake! |
| ④ | $C_6^1$ | 4 | | 2 | 0 | Legitimate | | 2 | 18 | Fake! | | 2 | 14 | Fake! |
| | | | | 3 | 0 | Legitimate | | 3 | 19 | Fake! | | 3 | 6 | Fake! |
| | | | | 4 | 0 | Legitimate | | 4 | 24 | Fake! | | 4 | 44 | Fake! |
| ⑤ | $C_7^1$ | 3 | | 2 | 32 | Fake! | | 2 | 24 | Fake! | | 2 | 16 | Fake! |
| | | | | 3 | 18 | Fake! | | 3 | 24 | Fake! | | 3 | 13 | Fake! |

## 6. Discussion

Although we have demonstrated the effectiveness of SSLight through a rich set of experiments with real-world datasets, we still acknowledge some limitations of SSLight in practice.

First, SSLight is a data-drive solution for fake certificate detection. Its detection capability largely relies on the quality of the dataset that is used to train the SSLight. If the training set contains inaccurate

or even incorrect information, the effectiveness of SSLight may not be ensured. To overcome this challenge and to fetch a high-quality dataset for SSLight training, we propose a globally-distributed certificate hunter. The basic idea is to deploy a number of machines around the world. Each machine will run ZMap [25], which can scan the entire IPv4 space within 49 minutes, to collect certificates from all of the potential HTTPS services on the Internet. We then follow the idea of Perspectives [12] and consider that a certificate is valid if it belongs to the majority copies. In this way, we can mitigate the possibility of getting fake certificates in the training set.

Second, despite SSLight being an off-line approach, it may involve on-line activities for the downloaded and updated dataset. These on-line activities will introduce the risk of the dataset being corrupted. To avoid this risk, we can deploy a trusted third party. SSLight can only download and update its dataset from such a third party after necessary authentication. In this way, we should ensure the security of the trusted third party. Otherwise, SSLight will be avoided.

Third, we show the effectiveness of SSLight using a measure of the reduction factor, rather than the detection rate. We do this because the reduction factor can show the detection capability in a complete manner. That is, if we use the detection rate directly (just as the results we show in Table 2), we must focus on a subset of fake certificates and legitimate ones. This subset cannot represent how the fake certificates and legitimate ones are distributed well and, therefore, can only show the effectiveness of SSLight for specific cases. Unlike that, if we choose reduction factor, we can show the detection capability in general. It will not be affected by the specific cases we use and can show all of the possibilities of the fake certificates that SSLight can detect.

Fourth, in this paper, we focus on the evaluation of SSLight using the dataset [22], which is the first complete dataset released to the public and may contain the minimized fake certificates inside, because it is crawled immediately after the hacker's behavior has been detected. In this dataset, the hacker's impact is restricted, and the dataset contains minimized incorrect information. Therefore, this dataset is the most appropriate one that shows the effectiveness of SSLight in a fair manner. Despite that, we will also investigate the effectiveness of SSLight using other datasets, such as https://wiki.mozilla.org/CA:Problematic_Practices, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/ and https://www.linshunghuang.com/papers/mitm.pdf, in our future work. This further investigation can help to demonstrate the status of SSLight in worse cases.

## 7. Related Work

Trust is widely used to secure information networks in various research fields. Successful applications include mobile *ad hoc* networks [26], wireless sensor networks [27], social networks [28], multi-agent networks [29] and, the most recent, anonymity networks [30,31]. These successful applications confirm the effectiveness and necessity of trust for network security. This paper's scope falls into the web systems. In the following, we will survey the related works that use trust or trust-like methods to avoid fake certificates in the web.

Perspective [12] is a pioneering work to identify fake certificates. To address the security vulnerability in the so-called trust-in-first-use authentication scheme, Perspective proposed to deploy a distributed

system around the world to help browsers obtain a legitimate sample of certificates. The basic idea of this project is adopted by HTTPS Everywhere [13] and Google Certificate Catalog [14], both of which provide on-line services to help users detect fake certificates issued from compromised CAs. However, these solutions need additional network communications, thus making them vulnerable to being blocked or hijacked. Certified Lies [4], on the other hand, focuses on the fake certificates issued by a special group of compromised CAs, the CAs that are compelled by governments. Although its solution is lightweight and does not need on-line checking, it operates in an *ad hoc* manner to address a limited number of attack scenarios and requires human interaction. The Sovereign Keys Project [15] provides a systematical solution to eliminate this security threat. However, The Sovereign Keys system introduces a totally different architecture, thus making it hard to replace the existing infrastructure in a short time.

The collection of legitimate HTTPS certificates has been done in several projects. However, some of them only focus on a specific target. For example, Lee *et a*l. [32] collected the legitimate samples to evaluate the certificates' cryptographic strength, and Yilek *et al*. [33] just paid attention to an OpenSSL vulnerability in the Debian system. The SSL Observatory project [6,34,35], according to our knowledge, is the first thorough collection and analysis of legitimate certificates. This project scans all of the allocated IPv4 space with the 443 port. SSL Landscape [36], on the other hand, provides another thorough collection of legitimate samples, but it focuses on the survey of high ranked HTTPS web servers. Both of the datasets from SSL Observatory and SSL Landscape can be used as a legitimate sample set in SSLight.

As browsers always allow users to make the final decision about whether the certificates are trustworthy or not, attacks targeted at the human interface are usually launched to compromise HTTPS connections. Many mechanisms have been proposed to mitigate this threat. For example, SSLock [37] intelligently makes the final decision on behalf of users. Adelsbach *et al.* [38] and Xia *et al.* [39] improved the human interface to make users be clearly aware when suspicious certificates are detected by browsers.

## 8. Conclusions

In this paper, we have proposed SSLight, a novel fake certificate detection mechanism based on attribute dependency. SSLight is demonstrated to be able to detect fake certificates issued from trusted, but compromised, CAs with a relatively low false positive. In particular, SSLight shows its practicability to expose the real-world fake certificates issued by DigiNotar and Comodo. Although the design of SSLight is only for HTTPS applications, this attribute dependency-based detection method can be extended to other SSL-/TLS-based applications and protocols.

## Acknowledgments

The work was supported by the National Natural Science Foundation of China under Grant No. 61205017 and the Fundamental Research Funds for the Central Universities.

## Author Contributions

The author Xiaojing Gu designed the research, perform the experiments, analysis the data and write most of the manuscript. The co-author Xingsheng Gu discusses the original idea and gives many constructive comments. Both the authors have read and approved the final manuscript.

## A. Appendix

### *1.1. The Proof of Proposition 2*

**Proof.** According to Equation (4), we have:

$$\begin{aligned}\sum_{V_k^{J_x,I_x}\in\mathbb{V}_{J_x}^{I_x}} Pr\{V_k^{J_x,I_x}|V_{K_y}^{J_y,I_y}\} &= \sum_{V_k^{J_x,I_x}\in\mathbb{V}_{J_x}^{I_x}} \frac{||\mathbb{C}(I_x,J_x,k)\bigcap\mathbb{C}(I_y,J_y,K_y)||}{||\mathbb{C}(I_y,J_y,K_y)||}\\ &= \frac{\sum\limits_{V_k^{J_x,I_x}\in\mathbb{V}_{J_x}^{I_x}} ||\mathbb{C}(I_x,J_x,k)\bigcap\mathbb{C}(I_y,J_y,K_y)||}{||\mathbb{C}(I_y,J_y,K_y)||}\\ &= \frac{||(\bigcup\limits_{V_k^{J_x,I_x}\in\mathbb{V}_{J_x}^{I_x}} \mathbb{C}(I_x,J_x,k))\bigcap\mathbb{C}(I_y,J_y,K_y)||}{||\mathbb{C}(I_y,J_y,K_y)||}.\end{aligned}$$

As $\bigcup\limits_{V_k^{J_x,I_x}\in\mathbb{V}_{J_x}^{I_x}} \mathbb{C}(I_x,J_x,k) = \mathbb{C} and \mathbb{C}(I_y,J_y,K_y)\subseteq\mathbb{C}$,

$$\Rightarrow \sum_{V_k^{J_x,I_x}\in\mathbb{V}_{J_x}^{I_x}} Pr\{V_k^{J_x,I_x}|V_{K_y}^{J_y,I_y}\} = \frac{||\mathbb{C}\bigcap\mathbb{C}(I_y,J_y,K_y)||}{||\mathbb{C}(I_y,J_y,K_y)||} = \frac{||\mathbb{C}(I_y,J_y,K_y)||}{||\mathbb{C}(I_y,J_y,K_y)||} = 1.$$

□

### *1.2. The Proof of Corollary 1*

**Proof.** According to Equation (9), we have:

$$R(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = \frac{||\mathbb{V}_{J_x}^1||}{||\mathbb{V}_{J_x}^{1+}(P_{th},A_{J_y}^{I_y,e})||}.$$

As $0\le||\mathbb{V}_{J_x}^{1+}(P_{th},A_{J_y}^{I_y,e})||\le||\mathbb{V}_{J_x}^1||$,

$$\Rightarrow 1\le R(P_{th}, D(A_{J_x}^1|V(A_{J_y}^{I_y,e})))\le\infty.$$

□

**Proof.** If $R(P_{th}<1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e})))=\infty$,

$$\begin{aligned}&\Rightarrow \quad ||\mathbb{V}_{J_x}^{1+}(P_{th}<1,A_{J_y}^{I_y,e})||=0,\\ &\Rightarrow \quad \mathbb{V}_{J_x}^{1-}(P_{th}<1,A_{J_y}^{I_y,e})=\mathbb{V}_{J_x}^1.\end{aligned}$$

$$\Rightarrow \sum_{V_k^{J_x,1}\in\mathbb{V}_{J_x}^1} Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} = \sum_{V_k^{J_x,1}\in\mathbb{V}_{J_x}^{1-}(P_{th}<1,A_{J_y}^{I_y,e})} Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\}$$
$$\leq \frac{P_{th}\times||\mathbb{V}_{J_x}^{1-}(P_{th}<1,A_{J_y}^{I_y,e})||}{||\mathbb{V}_{J_x}^1||} = P_{th} < 1.$$

However, according to Proposition 2,

$$\sum_{V_k^{J_x,1}\in\mathbb{V}_{J_x}^1} Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} = 1.$$

$$\begin{aligned}
&\Rightarrow \quad R(P_{th}<1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \neq \infty,\\
&\Rightarrow \quad ||\mathbb{V}_{J_x}^{1+}(P_{th}<1, A_{J_y}^{I_y,e})|| \geq 1,\\
&\Rightarrow \quad 1 \leq R(P_{th}<1, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \leq ||\mathbb{V}_{J_x}^1||.
\end{aligned}$$

□

### *1.3. The Proof of Corollary 2*

**Proof.** According to Equation (10), we have:

$$R^*(P_{th}, C_e^{I_y>1}) = \prod_{A_{J_x}^1\in\mathbb{A}^1} \frac{||\mathbb{V}_{J_x}^1||}{||\bigcap\limits_{A_{J_y}^{I_y}\in\mathbb{A}^{I_y}} \mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e})||}.$$

As $0 \leq ||\bigcap\limits_{A_{J_y}^{I_y}\in\mathbb{A}^{I_y}} \mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e})|| \leq ||\mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e})||$,

$$\begin{aligned}
&\Rightarrow \quad 0 \leq ||\bigcap_{A_{J_y}^{I_y}\in\mathbb{A}^{I_y}} \mathbb{V}_{J_x}^{1+}(P_{th}, A_{J_y}^{I_y,e})|| \leq ||\mathbb{V}_{J_x}^1||,\\
&\Rightarrow \quad 1 \leq R^*(P_{th}, C_e^{I_y>1}) \leq \infty.
\end{aligned}$$

□

**Proof.** If $P_{th} = 0 < 1$, based on Corollary 1's proof,

$$\begin{aligned}
&\Rightarrow \quad \exists A_{J_y}^{I_y} \in \mathbb{A}^{I_y}, ||\mathbb{V}_{J_x}^{1+}(P_{th}=0, A_{J_y}^{I_y,e})|| \geq 1,\\
&\Rightarrow \quad \exists A_{J_y}^{I_y} \in \mathbb{A}^{I_y}, \exists V_k^{J_x,1} \in \mathbb{V}_{J_x}^{1+}(P_{th}=0, A_{J_y}^{I_y,e}),
\end{aligned}$$

$Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} > \frac{P_{th}}{||\mathbb{V}_{J_x}^1||} = 0.$

According to the definition of $Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\}$ in Equations (3) and (4), when $Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} > 0$,

$$\Rightarrow \quad \exists\Gamma(C_e^1) \in \mathbb{C}, \quad \text{where } C_e^{I_y>1} \in \Gamma(C_e^1), V(A_{J_x}^{1,e}) = V_k^{J_x,1},$$

$$Pr\{V(A_{J_x}^{1,e})|V(A_{J_y}^{I_y,e})\} > 0 for \forall A_{J_y}^{I_y} \in \mathbb{A}^{I_y},$$
$$\Rightarrow \quad V(A_{J_x}^{1,e}) \in \mathbb{V}_{J_x}^{1+}(P_{th}=0, A_{J_y}^{I_y,e}) for \forall A_{J_y}^{I_y} \in \mathbb{A}^{I_y},$$
$$\Rightarrow \quad V(A_{J_x}^{1,e}) \in \bigcap_{A_{J_y}^{I_y} \in \mathbb{A}^{I_y}} \mathbb{V}_{J_x}^{1+}(P_{th}=0, A_{J_y}^{I_y,e}),$$
$$\Rightarrow \quad || \bigcap_{A_{J_y}^{I_y} \in \mathbb{A}^{I_y}} \mathbb{V}_{J_x}^{1+}(P_{th}=0, A_{J_y}^{I_y,e})|| \geq 1,$$
$$\Rightarrow \quad 1 \leq R^*(P_{th}=0, C_e^{I_y>1}) \leq \prod_{A_{J_x}^1 \in \mathbb{A}^1} ||\mathbb{V}_{J_x}^1||.$$

□

### *1.4. The Proof of Corollary 3*

**Proof.** If $R(P_{th} > 0, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \neq \infty$,

$$\Rightarrow \exists A_{J_y}^{I_y} \in \mathbb{A}^{I_y}, \exists V_k^{J_x,1} \in \mathbb{V}_{J_x}^{1+}(P_{th} > 0, A_{J_y}^{I_y,e}),$$

$Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} > \frac{P_{th}}{||\mathbb{V}_{J_x}^1||} > 0.$

$$\Rightarrow \exists \Gamma(C_e^1) \in \mathbb{C}, \text{ where } \quad C_e^{I_y>1} \in \Gamma(C_e^1), V(A_{J_x}^{1,e}) = V_k^{J_x,1},$$

$Pr\{V(A_{J_x}^{1,e})|V(A_{J_y}^{I_y,e})\} > 0$ for $\forall A_{J_y}^{I_y} \in \mathbb{A}^{I_y}$.

However, as $P_{th} > 0$, we cannot guarantee that the $\Gamma(C_e^1)$ with $V(A_{J_x}^{1,e}) = V_k^{J_x,1}$ results in $Pr\{V(A_{J_x}^{1,e})|V(A_{J_y}^{I_y,e})\} > \frac{P_{th}}{||\mathbb{V}_{J_x}^1||}$ for $\forall A_{J_y}^{I_y} \in \mathbb{A}^{I_y}$,

$\therefore \bigcap_{A_{J_y}^{I_y} \in \mathbb{A}^{I_y}} \mathbb{V}_{J_x}^{1+}(P_{th} > 0, A_{J_y}^{I_y,e}) = \varnothing$ is possible,

we may still have $R^*(P_{th} > 0, C_e^{I_y>1}) = \infty$ even if $\forall A_{J_x}^1 \in \mathbb{A}^1, \forall A_{J_y}^{I_y} \in \mathbb{A}^{I_y}, R(P_{th} > 0, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) \neq \infty$. □

### *1.5. The Proof of Corollary 4*

**Proof.** When $P_{th} = 0$, $\Rightarrow \forall V_k^{J_x,1} \in \mathbb{V}_{J_x}^{1-}(P_{th} = 0, A_{J_y}^{I_y,e})$, $Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} = 0$ and $\mathbb{C}(1, J_x, k) \bigcap \mathbb{C}(I_y, J_y, k') = \varnothing$, where $V(A_{J_y}^{I_y,e}) = V_{k'}^{J_x,I_x}$.

$$\Rightarrow E(P_{th}=0, D(A_{J_x}^1|V(A_{J_y}^{I_y,e}))) = \sum_{V_k^{J_x,1} \in \mathbb{V}_{J_x}^{1-}(P_{th}, A_{J_y}^{I_y,e})} Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} = 0.$$

According to Equation (12), we have:

$$\mathbb{C}(1, J_x, k) \bigcap \mathbb{C}(I_y, J_y, k') = \varnothing$$
$$\Rightarrow \quad \mathbb{C}_{J_x}^- \bigcap \mathbb{C}(I_y, J_y, k') = \varnothing$$
$$\Rightarrow \quad E^*(0, C_e^{I_y>1}) = 0.$$

□

### *1.6. The Proof of Corollary 5*

**Proof.** $R(P_{th} \geq 1, D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) = \infty$,

$$\begin{aligned} &\Leftrightarrow \ \mathbb{V}^{1+}_{J_x}(P_{th} \geq 1, A^{I_y,e}_{J_y}) = \varnothing, \\ &\Leftrightarrow \ \mathbb{V}^{1-}_{J_x}(P_{th} \geq 1, A^{I_y,e}_{J_y}) = \mathbb{V}^{1}_{J_x}, \\ &\Leftrightarrow \ E(P_{th} \geq 1, D(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) = 1. \end{aligned}$$

□

### *1.7. The Proof of Corollary 6*

**Proof.** $R^*(P_{th} \geq 1, C_e^{I_y>1}) = \infty$,

$$\begin{aligned} &\Rightarrow \bigcap_{A^{I_y}_{J_y} \in \mathbb{A}^{I_y}} \mathbb{V}^{1+}_{J_x}(P_{th} \geq 1, A^{I_y,e}_{J_y}) = \varnothing, \\ &\Rightarrow \bigcup_{A^{I_y}_{J_y} \in \mathbb{A}^{I_y}} \mathbb{V}^{1-}_{J_x}(P_{th} \geq 1, A^{I_y,e}_{J_y}) = \mathbb{V}^{1}_{J_x}, \\ &\Rightarrow \forall \Gamma(C^1_q) \in \mathbb{C}, V(A^{1,q}_{J_x}) \in \bigcup_{A^{I_y}_{J_y} \in \mathbb{A}^{I_y}} \mathbb{V}^{1-}_{J_x}(P_{th} \geq 1, A^{I_y,e}_{J_y}), \\ &\Rightarrow \forall \Gamma(C^1_q) \in \mathbb{C}, \exists A^{I_y}_{J_y} \in \mathbb{A}^{I_y}, \end{aligned}$$

$$Pr\{V(A^{1,q}_{J_x})|V(A^{I_y,e}_{J_y})\} \leq \frac{P_{th}}{||\mathbb{V}^1_{J_x}||}, \Rightarrow E^*(P_{th} \geq 1, C_e^{I_y>1}) = 1.$$

□

**Proof.** $E^*(P_{th} \geq 1, C_e^{I_y>1}) = 1$,

$$\Rightarrow \forall \Gamma(C^1_q) \in \mathbb{C}, V(A^{1,q}_{J_x}) \in \bigcup_{A^{I_y}_{J_y} \in \mathbb{A}^{I_y}} \mathbb{V}^{1-}_{J_x}(P_{th} \geq 1, A^{I_y,e}_{J_y}),$$

$\because$ it is possible that

$$\exists \Gamma(C^1_e) \notin \mathbb{C}, V(A^{1,e}_{J_x}) \in \bigcap_{A^{I_y}_{J_y} \in \mathbb{A}^{I_y}} \mathbb{V}^{1+}_{J_x}(P_{th} \geq 1, A^{I_y,e}_{J_y}),$$

$\therefore$

$$\begin{aligned} &\nRightarrow \bigcup_{A^{I_y}_{J_y} \in \mathbb{A}^{I_y}} \mathbb{V}^{1-}_{J_x}(P_{th} \geq 1, A^{I_y,e}_{J_y}) = \mathbb{V}^{1}_{J_x}, \\ &\nRightarrow R^*(P_{th} \geq 1, C_e^{I_y>1}) = \infty. \end{aligned}$$

□

### *1.8. An Example of Excluded Attribute Dependencies*

See Table 3.

**Table 3.** Excluded features $E(P_{th} = 1, D(A^1_{J_x}|V^{I_y,J_y}_{K_y})) > 0.15$. CA, certificate authority.

| $A^{I_y}_{J_y}$ | $I_y$ | $V^{I_y,J_y}_{K_y}$ | $A^1_{J_x}$ | $E$ |
|---|---|---|---|---|
| CommonName | 2 | UTN-USERFirst-Hardware | Locality | 0.154 |
| Locality | 2 | Salt Lake City | Locality | 0.185 |
| Organization | 2 | The USERTRUSTNetwork | Locality | 0.185 |
| OrganizationUnit | 2 | http://www.usertrust.com | Locality | 0.153 |
| StateOrProvince | 2 | UT | Locality | 0.185 |
| Description | 2 | EMPTY | Organization | 0.707 |
| PublicKeyAlgorithm | 2 | RSA | Organization | 0.702 |
| Country | 2 | ZA | OrganizationUnit | 0.159 |
| CommonName | 2 | Thawte Premium Server CA/emailAddress | OrganizationUnit | 0.191 |
| CommonName | 2 | DigiCert High Assurance CA-3 | OrganizationUnit | 0.151 |
| CommonName | 3 | DigiCert High Assurance EV Root CA | OrganizationUnit | 0.151 |
| Organization | 3 | DigiCert Inc | OrganizationUnit | 0.151 |
| OrganizationUnit | 3 | www.digicert.com | OrganizationUnit | 0.151 |
| Description | 3 | EMPTY | Organization | 0.709 |
| PublicKeyAlgorithm | 3 | RSA | Organization | 0.709 |
| Country | 3 | SE | Locality | 0.175 |
| CommonName | 3 | AddTrust External CA Root | Locality | 0.175 |
| Organization | 3 | AddTrust AB | Locality | 0.175 |
| OrganizationUnit | 3 | AddTrust External TTPNetwork | Locality | 0.175 |

### *1.9. The Proof of Proposition 3*

**Proof.** According to Equation (8), we have:
if $V^{J_x}_k \in \mathbb{V}^+_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))$,

$$|Pr\{V^{J_x,1}_k|V(A^{I_y,e}_{J_y})\} - \frac{P_{th}}{||\mathbb{V}_{J_x}||}| = Pr\{V^{J_x,1}_k|V(A^{I_y,e}_{J_y})\} - \frac{P_{th}}{||\mathbb{V}_{J_x}||},$$

if $V^{J_x}_k \in \mathbb{V}^-_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))$,

$$|Pr\{V^{J_x,1}_k|V(A^{I_y,e}_{J_y})\} - \frac{P_{th}}{||\mathbb{V}_{J_x}||}| = \frac{P_{th}}{||\mathbb{V}_{J_x}||} - Pr\{V^{J_x,1}_k|V(A^{I_y,e}_{J_y})\}.$$

As a result,

$$\begin{aligned}
\Rightarrow \phi(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) &= \sum_{V_k^{J_x} \in \mathbb{V}_{J_x}} |Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\} - \frac{P_{th}}{||\mathbb{V}_{J_x}||}| \\
&= \sum_{V_k^{J_x} \in \mathbb{V}^+_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))} (Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\} - \frac{P_{th}}{||\mathbb{V}_{J_x}||}) \\
&\quad + \sum_{V_k^{J_x} \in \mathbb{V}^-_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))} (\frac{P_{th}}{||\mathbb{V}_{J_x}||} - Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\}) \\
&= \sum_{V_k^{J_x} \in \mathbb{V}^+_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))} (Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\}) \\
&\quad - \sum_{V_k^{J_x} \in \mathbb{V}^-_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))} (Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\}) \\
&\quad + \frac{P_{th} \times (||\mathbb{V}^-_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))|| - ||\mathbb{V}^+_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))||)}{||\mathbb{V}_{J_x}||}.
\end{aligned}$$

As $\sum_{\forall V_k^{J_x} \in \mathbb{V}^+_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))} Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\} + \sum_{\forall V_k^{J_x} \in \mathbb{V}^-_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))} Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\} = \sum_{\forall V_k^{J_x} \in \mathbb{V}^-_{J_x}} Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\} = 1$, and $||\mathbb{V}^+_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))|| + ||\mathbb{V}^-_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))|| = ||\mathbb{V}_{J_x}||$,

$$\begin{aligned}
\Rightarrow \phi(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) &= 1 - 2 \times \sum_{V_k^{J_x} \in \mathbb{V}^-_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))} (Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\}) \\
&\quad + \frac{P_{th} \times (||\mathbb{V}_{J_x}|| - 2 \times ||\mathbb{V}^+_{J_x}(P_{th}, V(A^{I_y,e}_{J_y}))||)}{||\mathbb{V}_{J_x}||}.
\end{aligned}$$

According to Equations (9) and (11), we have:

$$\begin{aligned}
\phi(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) &= 1 + P_{th} - 2 \times E(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) \\
&\quad - \frac{2 \times P_{th}}{R(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y})))}.
\end{aligned}$$

□

### *1.10. The Proof of Corollary 7*

**Proof.** According to Equation (13) and $|Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\} - \frac{P_{th}}{||\mathbb{V}_{J_x}||}| \geq 0$, we have:

$$\phi(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) \geq 0.$$

According to Equation (9) and Corollary 1, we have:

$$\begin{aligned}
E(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) &\geq 0, \\
\frac{1}{R(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y})))} &\geq \frac{1}{||\mathbb{V}_{J_x}||}.
\end{aligned}$$

By considering Proposition 3, we have:

$$\begin{aligned}\phi(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) &= 1 + P_{th} - 2 \times E(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) \\ &\quad - \frac{2 \times P_{th}}{R(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y})))} \\ &\leq 1 + P_{th} - \frac{2 \times P_{th}}{||\mathbb{V}_{J_x}||}.\end{aligned}$$

Therefore, we finally obtain:

$$0 \leq \phi(P_{th}, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) \leq 1 + P_{th} - \frac{2 \times P_{th}}{||\mathbb{V}_{J_x}||}.$$

□

### *1.11. The Proof of Corollary 8*

**Proof.** According to Equation (8), when $P_{th} = 0$, we have:

$$\forall V_k^{J_x,1} \in \mathbb{V}^-_{J_x}(0, V_{K_y}^{J_y,I_y}), Pr\{V_k^{J_x,1}|V_{K_y}^{J_y,I_y}\} \leq 0,$$

by considering $\forall V_k^{J_x,1} \in \mathbb{V}_{J_x}, Pr\{V_k^{J_x,1}|V_{K_y}^{J_y,I_y}\} \geq 0$, we have:

$$\forall V_k^{J_x,1} \in \mathbb{V}^-_{J_x}(0, V_{K_y}^{J_y,I_y}), Pr\{V_k^{J_x,1}|V_{K_y}^{J_y,I_y}\} = 0.$$

According to Equation (11), we thus have:

$$E(P_{th} = 0, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) = \sum_{\forall V_k^{J_x} \in \mathbb{V}^-_{J_x}(0, V(A^{I_y,e}_{J_y}))} Pr\{V_k^{J_x,1}|V(A^{I_y,e}_{J_y})\} \equiv 0.$$

As a consequence, according to Proposition 3, we have:

$$\phi(P_{th} = 0, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) \equiv 1.$$

□

### *1.12. The Proof of Corollary 9*

**Proof.** According to Corollary 7, when $P_{th} = 1$, we have:

$$0 \leq \phi(1, \mathbb{D}(A^1_{J_x}|V(A^{I_y,e}_{J_y}))) \leq 1 + 1 - \frac{2 \times 1}{||\mathbb{V}_{J_x}||} = \frac{2 \times (||\mathbb{V}_{J_x}|| - 1)}{||\mathbb{V}_{J_x}||}.$$

When $\phi(1, \mathbb{D}(A^{I_x}_{J_x}|V(A^{I_y,e}_{J_y}))) = 0$, according to Equation (13),

$$\begin{aligned}&\Rightarrow \quad \forall V_k^{J_x} \in \mathbb{V}_{J_x}, |Pr\{V_k^{J_x,I_x}|V(A^{I_y,e}_{J_y})\} - \frac{1}{||\mathbb{V}_{J_x}||}| = 0, \\ &\Rightarrow \quad \forall V_k^{J_x} \in \mathbb{V}_{J_x}, Pr\{V_k^{J_x,I_x}|V(A^{I_y,e}_{J_y})\} = \frac{1}{||\mathbb{V}_{J_x}||}, \\ &\Rightarrow \quad \mathbb{D}(A^{I_x}_{J_x}|V(A^{I_y,e}_{J_y}))\end{aligned}$$

follows the uniform distribution.

When $\phi(1, \mathbb{D}(A_{J_x}^{I_x}|V_{K_y}^{J_y,I_y})) = \frac{2(||\mathbb{V}_{J_x}||-1)}{||\mathbb{V}_{J_x}||}$, according to Corollary 7, we have: $E(1, \mathbb{D}(A_{J_x}^{1}|V(A_{J_y}^{I_y,e}))) = 0$ and $||\mathbb{V}_{J_x}^{+}(1, V(A_{J_y}^{I_y,e}))|| = 1$,

$$\Rightarrow \exists V_k^{J_x,1} \in \mathbb{V}_{J_x}^{+}(1, V(A_{J_y}^{I_y,e})) \subseteq \mathbb{V}_{J_x},$$

$Pr\{V_k^{J_x,1}|V(A_{J_y}^{I_y,e})\} = 1$, $\Rightarrow$ a certain value of $A_{J_x}^{1}$ possesses the probability one.

□

## Conflicts of Interest

The authors declare no conflict of interest.

## References


1. Vatra, N. Public key infrastructure overview. *Sci. Stud. Res. Ser. Math. Inform.* **2009**, *19*, 471–478.
2. Solo, D.; Housley, R.; Ford, W. *Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*; The Internet Society: Reston, VA, USA, 2002.
3. Dierks, T. *The Transport Layer Security (TLS) Protocol Version 1.2*; The Internet Society: Reston, VA, USA, 2008.
4. Soghoian, C.; Stamm, S. Certified lies: Detecting and defeating government interception attacks against SSL (short paper). In *Financial Cryptography and Data Security*; Springer: Berlin, Germany, 2012; pp. 250–259.
5. Callegati, F.; Cerroni, W.; Ramilli, M. Man-in-the-middle attack to the HTTPS protocol. *IEEE Secur. Priv.* **2009**, *7*, 78–81.
6. Foundation, E.F. The EFF SSL Observatory. 2014. Available online: http://www.eff.org/observatory (accessed on 4 June 2015).
7. Foundation, E.F. The EFF Color Map of CAs. 2014. Available online: http://www.eff.org/files/colour_map_of_CAs.pdf (accessed on 4 June 2015).
8. Advisory, M.S. Fraudulent Digital Certificates Could Allow Spoofing. 2011. Available online: http://technet.microsoft.com/en-us/security/advisory/2607712 (accessed on 4 June 2015).
9. Nightingale, J. Diginotar Removal Follow Up. 2011. Available online: http://blog.mozilla.com/security/2011/09/02/diginotar-removal-follow-up/ (accessed on 4 June 2015).
10. Fisher, D. New Versions of Chrome and Firefox Disable Diginotar Root. 2011. Available online: https://threatpost.com/new-versions-chrome-and-firefox-disable-diginotar-root-083111/75600 (accessed on 4 June 2015).
11. M. S. Blog Comodo certificate issue follow up. 2011. Available online: https://blog.mozilla.com/security/2011/03/25/comodo-certificate-issue-follow-up/ (accessed on 4 June 2015).
12. Wendlandt, D.; Andersen, D.G.; Perrig, A. Perspectives: Improving SSH-style host authentication with multi-path probing. In Proceedings of the USENIX Annual Technical Conference, Boston, MA, USA, 22–27 June 2008; pp. 321–334.

13. Tor Project HTTPS Everywhere. 2011. Available online: https://trac.torproject.org/projects/tor/wiki/doc/HTTPSEverywhere/SSLObservatorySubmission(accessed on 4 June 2015).
14. Laurie, B. Improving SSL Certificate Security. 2011. Available online: http://googleonlinesecurity.blogspot.com/2011/04/improving-ssl-certificate-security.html (accessed on 4 June 2015).
15. Foundation, E.F. The Sovereign Keys Project. 2011. Available online: https://www.eff.org/zh-hans/sovereign-keys (accessed on 4 June 2015).
16. International Telecommunication Union. Information Technology ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). 2002. Available online: http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf (accessed on 4 June 2015).
17. International Telecommunication Union. Information Technology Open Systems Interconnection the Directory: Selected Attribute Types. 2002. Available online: http://www.itu.int/rec/T-REC-X.520-200811-I/en (accessed on 1 July 2012).
18. Nystrom, M.; Kaliski, B. Certification Request Syntax Specification Version 1.7. 2008. Available online: http://tools.ietf.org/html/rfc2986 (accessed on 4 June 2015).
19. Nightingale, J. Fraudulent *.google.com Certificate. 2011. Available online: http://blog.mozilla.com/security/2011/08/29/fraudulent-google-com-certificate/ (accessed on 4 June 2015).
20. Nightingale, J. Diginotar Removal Follow up. 2011. Available online: http://blog.mozilla.com/security/2011/09/02/diginotar-removal-follow-up/ (accessed on 4 June 2015).
21. Boneh, D. SSL Man in the Middle Proxy. 2007. Available online: http://crypto.stanford.edu/ssl-mitm/ (accessed on 4 June 2015).
22. Foundation, E.F. Observatory Certificate Database. 2007. Available online: http://www.eff.org/files/observatory-dec-2010.sql.lzma.torrent (accessed on 4 June 2015).
23. SSL MITM Attack by Iranian Government. 2011. Available online: http://pastebin.com/ff7Yg663 (accessed on 4 June 2015).
24. Comodo fraud incident. 2011. Available online: https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html (accessed on 4 June 2015).
25. Durumeric, Z.; Wustrow, E.; Halderman, J.A. ZMap: Fast Internet-wide scanning and its security applications. In Proceedings of the 22nd USENIX Security Symposium, Washington, DC, USA, 14–16 August 2013; pp. 605–620.
26. Cho, J.H.; Swami, A.; Chen, R. A survey on trust management for mobile ad hoc networks. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 562–583.
27. Zhou, P.; Jiang, S.; Irissappane, A.A.; Zhang, J.; Zhou, J.; Teo, J.C.M. Toward energy-efficient trust system through watchdog optimization for WSNs. *IEEE Trans. Inf. Forens. Secur.* **2015**. *10*, 613–625.
28. Eirinaki, M.; Louta, M.D.; Varlamis, I. A Trust-aware system for personalized user recommendations in social networks. *IEEE Trans. Syst. Man Cybern.* **2014**, *44*, 409–421.
29. Huynh, T.D.; Jennings, N.R.; Shadbolt, N.R. An integrated trust and reputation model for open multi-agent systems. *Autono. Agents Multi-Agent Syst.* **2006**, *13*, 119–154.
30. Zhou, P.; Luo, X.; Chen, A.; Chang, R.K. SGor: Trust graph based onion routing. *Comput. Netw.* **2013**, *57*, 3522–3544.

31. Zhou, P.; Luo, X.; Chang, R.K. Inference attacks against trust-based onion routing: Trust degree to the rescue. *Comput. Secur.* **2013**, *39*, 431–446.
32. Lee, H.K.; Malkin, T.; Nahum, E. Cryptographic strength of SSL/TLS servers: Current and recent practices. In Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, San Diego, CA, USA, 24–26 October 2007; pp. 83–92.
33. Yilek, S.; Rescorla, E.; Shacham, H.; Enright, B.; Savage, S. When private keys are public: Results from the 2008 Debian OpenSSL vulnerability. In Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement, Chicago, IL, USA, 4–6 November 2009; pp. 15–27.
34. Ristic, I. Internet SSL survey 2010. Available online: http://media.blackhat.com/bh-us-10/presentations/Ristic/BlackHat-USA-2010-Ristic-Qualys-SSL-Survey-HTTP-Rating-Guide-slides.pdf (accessed on 4 June 2015).
35. Eckersley, P.; Burns, J. Is the SSLiverse a Safe Place? 2010. Available online: http://www.eff.org/files/ccc2010.pdf (accessed on 4 June 2015).
36. Holz, R.; Braun, L.; Kammenhuber, N.; Carle, G. The SSL landscape: A thorough analysis of the X.509 PKI using active and passive measurements. In Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, Berlin, Germany, 2–4 November 2011; pp. 427–444.
37. Fung, A.P.; Cheung, K. SSLock: Sustaining the trust on entities brought by SSL. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, 13–16 April 2010; pp. 204–213.
38. Adelsbach, A.; Gajek, S.; Schwenk, J. Visual spoofing of SSL protected web sites and effective countermeasures. In *Information Security Practice and Experience*; Springer: Berlin, Germany, 2005; pp. 204–216.
39. Xia, H.; Brustoloni, J.C. Hardening web browsers against man-in-the-middle and eavesdropping attacks. In Proceedings of the 14th International Conference on World Wide Web, Chiba, Japan, 10–14 May 2005; pp. 489–498.