Applied Mathematics and Computation 333 (2018) 467–479

Contents lists available at ScienceDirect

Applied Mathematics and Computation

journal homepage: www.elsevier.com/locate/amc

Still wrong use of pairings in cryptography

Osmanbey Uzunkol[a,b,*], Mehmet Sabır Kiraz[b]

[a] FernUniversität in Hagen, Fakulty of Mathematics and Computer Science, Universitätsstr. 1 (IZ), D-58097 Hagen, Germany
[b] Mathematical and Computational Sciences Labs, TÜBİTAK BİLGEM, P.O. BOX: 74, 41470, Gebze/Kocaeli, Turkey

ARTICLE INFO

MSC:
94A60

Keywords:
Pairing-based protocols
Bilinear maps
Security
Efficiency
The discrete logarithm problem

ABSTRACT

Recently many pairing-based cryptographic protocols have been designed with a wide variety of new novel applications including the ones in the emerging technologies like cloud computing, internet of things (IoT), e-health systems, and wearable technologies. There have been, however, a wide range of incorrect use of these primitives mainly because of their use in a “black-box” manner. Some new attacks on the discrete logarithm problem lead to either totally insecure or highly inefficient pairing-based protocols, and extend considerably the issues related to pairings originally pointed out by Galbraith et al. (2008). Other reasons are the implementation attacks, the minimal embedding field attacks, and the issues due to the existence of auxiliary inputs. Although almost all these issues are well-known to mathematical cryptographers, there is no state-of-the-art assessment covering all these new issues which could be used by the applied cryptography researchers and the IT-security developers. In order to illustrate this point, we give a list of recent papers having either wrong security assumptions or realizability/efficiency issues. Furthermore, we give a compact and an state-of-the-art recipe of the correct use of pairings for the correct design with a view towards efficient and secure implementation of security solutions using these primitives.

1. Introduction

Pairing-based cryptography has received much attention because of wide variety of its immediately deployable applications. These applications include identity-based encryption, functional and attribute-based encryption, searchable encryption, short/group/ring signatures, signcryption, homomorphic linear authenticators for integrity checking, security, privacy and integrity solutions for cloud computing and Internet of Things (IoT), e-health systems, and wearable technologies. We refer to Appendix for a selected list of some novel applications using pairing-based cryptography. In practice, Voltage Security (now an HP company) and Trend Micro are the most well-known companies utilizing the pairing-based security solutions [66].

There have been unfortunately a collection of recent results using the pairings incorrectly due to not being aware of the recent advancements on solving the discrete logarithm problems in some groups. We observed that there are unfortunately plenty of very recently introduced papers (surprisingly) either having pairing related wrong security assumptions and/or efficiency issues.

[*] Corresponding author at: FernUniversität in Hagen, Fakulty of Mathematics and Computer Science, Universitätsstr. 1 (IZ), D-58097 Hagen, Germany.
E-mail addresses: osmanbey.uzunkol@gmail.com, osmanbey.uzunkol@fernuni-hagen.de (O. Uzunkol), mehmet.kiraz@tubitak.gov.tr (M.S. Kiraz).

https://doi.org/10.1016/j.amc.2018.03.062
0096-3003/© 2018 Elsevier Inc. All rights reserved.

The security of pairing-based cryptosystems relies on the difficulty of various computationally hard problems related to the discrete logarithm problem (DLP). The new attacks on the DLP on some groups [3,9,37,39,69] have significant consequences on the security of some pairings primitives. Furthermore, very recent results on solving the DLP for finite fields of medium characteristics and composite degrees size have also consequences on the choice of key sizes for pairing based cryptography [8,45,48,72]. Hence, ignoring these recent technical advancements in solving the DLP make certain security assumptions incorrect. We note that although some basic problems related to using pairings as "black boxes" incorrectly was introduced by Galbraith et al. [35], not being aware of of these new issues is the primary reason of designing protocols which have considerably critical security vulnerabilities, realizability issues and/or efficiency problems. The complexity of these mathematical preliminaries is undoubtedly the reason of neglecting the realization concerns in the design of pairing-based protocols.

1.1. Our contribution

The main contributions can be listed as follows:

- Firstly, we highlight the main issues related to the correct use of pairings by revisiting the most recent attacks against pairing-based cryptography. These include new advancements in the discrete logarithm problem, implementation attacks, and others (e.g., protocols based on the discrete logarithm problem with auxiliary inputs, minimum embedding degree attacks).
- We give secondly a new assessment of the correct use of pairings with an informative and less technical way (as a recipe for designers and developers) extending considerably the issues already introduced by Galbraith et al. [35]. Thereby, we show the serious effects of the recent attacks on the designs, security models, and hardness assumptions of cryptographic protocols related to efficient and secure realization of pairing-based real-world applications.
- Following the lines of our assessment, we present security and/or efficiency issues of many recent papers. In particular, some of these issues could easily be solved by using smaller key but larger ciphertext sizes whereas the others unfortunately nullify the contribution because of unrealizable and/or insecure use of pairings.

2. Basics for pairing-based cryptography

We begin with the abstract pairing requirements and different types of bilinear maps used in cryptographic protocols.

Let $(\mathbf{G}_1, +)$ and $(\mathbf{G}_2, +)$ be two additive cyclic groups of (nearly) prime order q with $\mathbf{G}_1 =< P >$ and $\mathbf{G}_2 =< Q >$, $(\mathbf{G}_T,\cdot)$ be a multiplicative cyclic group of order q with $\mathbf{G}_T =< g >$. We write as usual 0 for the identity elements of $\mathbf{G}_1$, $\mathbf{G}_2$ and 1 for $\mathbf{G}_T$. A *pairing* or a *bilinear map* is a map $e: \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$ satisfying the following properties:

- *Bilinearity:* For all $P_1, P_1' \in \mathbf{G}_1, Q_1, Q_1' \in \mathbf{G}_2$, e is a group homomorphism in each component, i.e.
  1. $e(P_1 + P_1', Q_1) = e(P_1, Q_1) \cdot e(P_1', Q_1)$,
  2. $e(P_1, Q_1 + Q_1') = e(P_1, Q_1) \cdot e(P_1, Q_1')$.
- *Non-degeneracy:* e is non-degenerate in each component, i.e.
  1. For all $P_1 \in \mathbf{G}_1$, $P_1 \neq 0$, there is an element $Q_1 \in \mathbf{G}_2$ such that $e(P_1, Q_1) \neq 1$,
  2. For all $Q_1 \in \mathbf{G}_2$, $Q_1 \neq 0$, there is an element $P_1 \in \mathbf{G}_1$ such that $e(P_1, Q_1) \neq 1$.
- *Computability:* There exists an algorithm which computes the bilinear map e efficiently.

There are essentially 4 types of bilinear maps [35,74] used in the design of pairing-based protocols depending on the special requirements such as short representation, hashing to a group element, efficient homomorphisms.

- *Type-1:* $\mathbf{G}_1 = \mathbf{G}_2$. In this case there exists no short representations for the elements of $\mathbf{G}_1$.
- *Type-2:* $\mathbf{G}_1 \neq \mathbf{G}_2$ and there is an efficiently computable homomorphism ϕ: $\mathbf{G}_2 \to \mathbf{G}_1$. In this case no efficient secure hashing to the elements in $\mathbf{G}_2$ is possible.
- *Type-3:* $\mathbf{G}_1 \neq \mathbf{G}_2$ and there exists no efficiently computable homomorphism ϕ: $\mathbf{G}_2 \to \mathbf{G}_1$.
- *Type-4:* $\mathbf{G}_1 \neq \mathbf{G}_2$ and there exists an efficiently computable homomorphism ϕ: $\mathbf{G}_2 \to \mathbf{G}_1$ as in the case of the Type-2 setting but with an efficient secure hashing method to a group element [74]. Security proofs can be quite cumbersome in this setting as discussed in [50]. We note that this type is not generally used in protocol designs due to its inefficiency.

The main disadvantage of the Type-2 pairing is that there exists no random sampling algorithm from $\mathbf{G}_2$ (yielding to a secure hash function) which maps arbitrary elements to $\mathbf{G}_2$, [35, pp. 3119]. Note that there exists a natural, efficient, and secure transformation of protocols using the Type-2 pairing into protocols using the Type-3 pairing [18, Section 5]. We summarize this fact as follows since we need this in the subsequent sections:

Fact 1. For Type-2 pairings there exists no random sampling algorithm from $\mathbf{G}_2$ mapping arbitrary elements into $\mathbf{G}_2$. Therefore, Type-2 pairings cannot have secure hash functions into the group $\mathbf{G}_2$.

Remark 1. We note that most pairing-based aggregate signature protocols require an efficiently computable homomorphism ϕ: $\mathbf{G}_2 \to \mathbf{G}_1$, i.e., they use pairings of Type-2, see for instance [15].

The Type-1 setting is commonly called *symmetric pairing* while other types are called *asymmetric pairing*.

Properties and conversion of types. Since the situation $\mathbf{G}_1 \neq \mathbf{G}_2$ with efficiently computable homomorphisms (in both directions) is essentially the same with the Type-1 setting (by identifying the groups via explicit homomorphisms), we do not consider it separately.

The main technical part of pairing-based cryptography is the pairing functions including Weil, Tate and Ate pairing defined mostly on the product of certain subgroups of low dimensional abelian varieties over finite fields (in practice either on subgroups of elliptic curves or jacobians of genus two hyperelliptic curves) [11].

Due to efficiency and realizability concerns of pairing-based protocols many ad hoc and conceptual conversion methods from one type of pairing to another one has been proposed [21,71,82]. Abe et al. [2] proposed a generic framework converting not only the protocols with the Type-1 bilinear maps into the Type-3 setting but also converting corresponding security proofs using black-box reduction methods in the random oracle model. Akinyele et al. [4] have very recently given some concerns about the practicability of the elegant theoretic solution of [2] and proposed an automated software tool transforming schemes using the Type-1 bilinear maps into the Type-3 setting. We note however that the proposed automated tool in [4] and generic frameworks in [2] suffer from being inefficient when compared to their manual counterparts like [21,71,82]. In [4,p. 20], it is left as an open problem to generalize and systematize the manual advancement more efficiently for automated tools.

Basic computational problems related to pairing. For completeness of the paper, we briefly summarize the basic computational problems. Let $\mathbf{G}$ be a finite cyclic group of order n and $P \in \mathbf{G}$ be its generator (here additively written). In order to use $\mathbf{G}$ for cryptographic purposes, we need the existence of the efficient algorithms available to compute in the group $\mathbf{G}$. Hence, the isomorphism between $(\mathbb{Z}/n\mathbb{Z}, +)$ and $(\mathbf{G}, +)$ can explicitly be given and efficiently computable via

$$\phi: \ \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbf{G}, \ \ a \mapsto aP.$$

The discrete logarithm problem (DLP) asks to find the preimage in $\mathbb{Z}/n\mathbb{Z}$ of an arbitrarily chosen element in $\mathbf{G}$, i.e. to find a for a given pair (P, aP), where a is chosen randomly in $\mathbb{Z}/n\mathbb{Z}$. If the DLP is not intractable, in other words, if one can efficiently compute $\phi^{-1}(Q)$ for any $Q \in \mathbf{G}$, then all pairing related hardness assumptions will be wrong, i.e. they cannot be used to design secure cryptographic protocols.

The computational Diffie–Hellman problem is to compute abP for a given triple (P, aP, bP) where a, b are chosen randomly in $\mathbb{Z}/n\mathbb{Z}$. The decisional Diffie–Hellman problem is to decide $Q \overset{?}{=} abP$ for a given quadruple (P, aP, bP, Q) where a, b are chosen randomly in $\mathbb{Z}/n\mathbb{Z}$. Due to Pohling–Hellman reduction it is usual to assume that $\mathbf{G}$ has a (nearly) prime order r (or has a large prime order subgroup of order r, respectively).

Provided that there exists a DLP solver for the image group $\mathbf{G}_T$ one has the following well-known fact by Frey-Rück and Menezes et al.:

Theorem 1. *[32,65] If there exists a bilinear map e: $\mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$, then the DLP in $\mathbf{G}_1$ and $\mathbf{G}_2$ can be solved in polynomial time in the number of digits if there exists a DLP oracle for $\mathbf{G}_T$.*

In the literature this attack is known as the MOV reduction attack. The result follows in a straightforward manner by the assumption that the pairing function e is efficiently computable: given $P \in \mathbf{G}_1$ and $aP \in \mathbf{G}_2$, we can compute $e(P, Q) \in \mathbf{G}_T$ and $e(P, aQ) = e(P, Q)^a \in \mathbf{G}_T$. Then the DLP solver for $\mathbf{G}_T$ can be used to obtain a [32,65].

3. Attacks on pairing-based cryptography

Several attacks on the DLP have recently been proposed improving the function field sieve algorithm in the multiplicative group of finite fields of small characteristics [3,9,37,39,69]. There are serious implications of these attacks on the security of pairing-based cryptography. More concretely, the use of symmetric pairing, and hence the use of pairing-friendly elliptic/hyperelliptic curves over fields of small characteristic are essentially useless [3,39]. Concrete attacks are performed for certain supersingular elliptic/hyperelliptic curves over $\mathbb{F}_2$ and $\mathbb{F}_3$, see [3,39]. Difficulties of generalizing these attacks on the elliptic curve setting are pointed out in a recent work of Massierer [64]. However, it can be argued more generally that the use of elliptic curves over finite fields of small characteristics in group-based cryptography has severe potential security threads. Especially, a very recent conjectural algorithm of Semaev [73] shows that the believed security level of 285 bits for a NIST elliptic curve over $\mathbb{F}_2^{571}$ can be reduced asymptotically to a security level of 101.7 bits using a variant of Weil descent attack although there is not a consensus on the validity of such asymptotical conjectures [33].

In this section we summarize the attacks on pairing-based cryptography together with their implications.

3.1. Recent advances in solving the DLP

The difficulty of the DLP depends on the description of the underlying group $\mathbf{G}$. Indeed, Shoup showed that the intractability of the DLP is closely related to the algorithms available to the description of $\mathbf{G}$. He further shows that in generic groups the computation of the discrete logarithms costs at least $\Omega(\sqrt{p})$, where p is the largest prime divisor of the

Table 1
Comparison with the recommended security levels for pairing groups, corresponding embedding degrees, ρ, and #of modular multiplications (MM) over the prime field $\mathbb{F}_r$ for Ate and twisted Ate pairing using Barreto–Naehrig curves, (groups $\mathbf{G}_1$ and $\mathbf{G}_2$ have the same prime order r, $\mathbf{G}_T$ is a subgroup of $\mathbb{F}_{q^k}$ of order r, k is the embedding degree which is the smallest integer such that $r|(q^k-1)$, i.e. k is the order of $q \mod r$) [67].

Security level (bits)	r (bits)	q^k (bits)	k with $\rho \approx 1$	Ate pairing ($k=12$)	Twisted Ate pairing ($k=12$)
80	160	960–1280	6–8	4647 MM	7800 MM
128	256	3000–5000	12–20	7119 MM	12,480 MM
192	384	7000–9000	18–24	17007 MM	31,200 MM
256	512	14,000–18,000	28–36	33486 MM	62,400 MM

order of **G** [76]. In particular, computing the discrete logarithms in generic groups requires approximately $\sqrt{p}$ computation in **G**. Recent advances on solving the DLP for finite fields have major consequences on the secure design of pairing based protocols. There are mainly two new attacks (1) quasi-polynomial DLP solver for small characteristics field, and (2) a more efficient variant of a DLP solver for medium characteristics fields of composite degree.

1. It was a well-known fact that the DLP for the multiplicative subgroups of finite fields is not as difficult as in the generic groups. However, many research have been done using these groups for cryptographic purposes by neglecting possible use of the algorithmic description of these groups to solve the discrete logarithm instances. The situation has been dramatically changed with the recent advancements of Barbulescu et al. [9] and Göloglu et al. [37]. Recently, Granger et al. [40] improved the result of Barbulescu et al. [9] by proposing a new expected quasi-polynomial algorithm for solving the DLP for finite fields $\mathbf{F}_q^k$ with roughly $q \approx k$. These attacks removed the DLP for multiplicative subgroups of small characteristic finite fields from the list of intractable problems.
2. Very recent results on a variant of the number field sieve algorithm for solving the discrete logarithm problem in medium characteristics finite fields of composite degrees have direct consequences on the choice of key sizes for pairing based algorithms [45,48,72]. The complexity analysis of these new techniques suggests that doubling the sizes of the underlying elliptic curves is a conservative choice of maintaining the desired security level. For possible proposals of new pairing-friendly curves of 128 and 192 bits of security we refer to the very recent result of Barbulescu and Duquesne [8].

Explicit realization of the bilinear maps can be done if $\mathbf{G}_T$ is a subgroup of the multiplicative group of a finite field. In particular, the DLP on $\mathbf{G}_1$ and $\mathbf{G}_2$ can be transferred into the subgroup of a finite field by Theorem 1. Hence, the algorithms for solving the DLP for finite fields are applicable on the discrete logarithm instances of pairing groups $\mathbf{G}_1$ and $\mathbf{G}_2$. Therefore, these new attacks have direct consequences on the security of many pairing-based cryptographic applications if the characteristic of the field defining $\mathbf{G}_1$ is small [47]. In fact, subsequent results applying the idea of this algorithm (combined with Frey-Rück and MOV attacks [26]) showed the fatal security issues for cryptographic protocols using the Type-1 bilinear maps [3,9,39,69].

In particular, for a group of size n with

$$L_n(\alpha, c) = \exp((c + o(1))(\log n)^{\alpha}(\log\log n)^{1-\alpha}),$$

where $0 < \alpha < 1, c > 0$, Barbulescu et al. [9] improved the previous bound for solving the DLP of Joux from $L_n(1/4)$ for a specified c to $n^{O(\log n)}$ for fields of the form $\mathbf{F}_q^k$ with roughly $q \approx k$. The key idea is to use a new and elegant approach for the descent phase.

3.1.1. Realization of bilinear maps

In order to understand the impact of these attacks on the design of pairing-based cryptographic protocols, we now briefly summarize the realization of bilinear maps using suitable elliptic curves for cryptographic purposes.

Over a finite field $\mathbb{F}_q$ with $q = p^m$, p a prime and $m \in \mathbb{N}$, the candidate groups $\mathbf{G}_1$ and $\mathbf{G}_2$ in the definition of bilinear maps are certain subgroups of a carefully chosen elliptic curve E over $\mathbb{F}_q$. In particular, $\mathbf{G}_1$ is the r-th torsion subgroup $E(\mathbb{F}_q)[r]$ and $\mathbf{G}_2$ is a certain group related to the explicit realization of the bilinear map. We refer to [11] for further details.

The abstract condition on the efficient computation of

$$e: \ \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$$

is realizable using Tate, Weil, Ate, and optimal pairing of elliptic curves, see for example [41]. More concretely, given an elliptic curve E over $\mathbb{F}_q$ the function e takes rational points of E over $\mathbb{F}_q$ or $\mathbb{F}_{q^k}$ as inputs and outputs elements of $\mathbb{F}^*_{q^k}$, where k is the smallest integer with the property that r divides $q^k - 1$. the value k is called the embedding degree of E with respect to r. To achieve the desired security and efficiency in $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_T$ the ratio $\log q^k / \log r = k\rho$ with $\rho = \log q / \log r$ has to be balanced. We refer to [30] for the details. For implementation and comparison purposes, one can consult Table 1 following the lines of [67].

The probability that a randomly chosen (nearly) prime order elliptic curve E has small enough embedding degree is negligibly small (generically k is in $O(q)$) [30,63]. Hence, special pairing-friendly curves have to be constructed in order to realize an efficiently computable function e with the property that the DLP is still intractable. Supersingular elliptic curves were initially the natural candidates of realizing such efficiently computable functions e with the desired security level. The reason was that supersingular elliptic curves have embedding degrees $k = 2, 4$ or 6 depending on whether $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$, $\mathrm{char}(\mathbb{F}_q) = 2$ and $\mathrm{char}(\mathbb{F}_q) = 3$, respectively [11]. We refer to [30] for further details on constructing curves with larger embedding degrees, i.e. the construction of ordinary pairing-friendly curves over prime fields with complex multiplication (CM) techniques (both families and individual curve constructions).

3.1.2. Consequences of the quasi-polynomial attacks on pairing-based cryptography

As briefly outlined above, the new attacks for solving the DLP on the multiplicative subgroup of small characteristic finite fields have also dramatic consequences for the design of pairing-based protocols. In fact, these attacks showed either the insecurity of the use of supersingular elliptic curves (all pairing-friendly elliptic curves over fields of characteristic 2 or 3) or the inefficiency of their usage (all supersingular curves defined over a large characteristic prime field) in the pairing-based settings [3,9,37,39,69]. Since the Type-1 pairing can only be realized using supersingular elliptic/hyperelliptic curves [35] we see in Section 4 that all Type-1 bilinear maps and the related protocols are either useless or regarded completely as insecure. The summary of these results is given with the following fact:

Fact 2. Type-1 pairings using supersingular elliptic curves over a finite field of characteristics 2 and 3 are completely insecure. Hence, current versions of the reports and standards of pairing-based cryptography (e.g., the report of NIST [66] and the standard of IEEE [1]) are required to be updated and the use of those curves needs to be forbidden. Furthermore, the use of Type-1 pairings using supersingular elliptic curves over finite fields of large characteristics (i.e., the embedding degree is 2) is highly inefficient when compared to the use of Type-3 pairings.

3.1.3. Consequences of the attacks for composite degree finite fields on pairing-based cryptography

The attack of Barbulescu and Kim [48] reduces the complexity of solving the DLP problem on $\mathbf{F}_p^n$ from $L_n(1/3, \sqrt[3]{96/9})$ to $L_n(1/3, \sqrt[3]{48/9})$ if $n = \kappa\eta$ with $\gcd(\kappa, \eta) = 1$ and $\kappa, \eta > 1$. Recently, Jeong and Kim removed the condition $\gcd(\kappa, \eta) = 1$ implying that if n is composite, the previous key sizes could be doubled asymptotically to guarantee the same security level of the discrete logarithm problem. Since, most pairing friendly elliptic curves have composite embedding degree (i.e. BN curves have embedding degree 12), one needs to be careful for the choice of elliptic curves, and to change their sizes according to these new attacks. Using a more conservative but less efficient elliptic curves of embedding degree one would also be an alternative to implement pairing-based protocols. For the choice and right notion of types of pairings of embedding degree one we refer to the recent article of Chattarjee et al. [20]. The following fact emphasizes that the current key sizes in the asymmetric setting, whence the speed estimations of pairing-based protocols, are required to be immediately updated for almost all pairing-based schemes in the literature:

Fact 3. Previous key size estimations are outdated for all pairings having composite embedding degree due to the attacks on the discrete logarithm problem for composite degree finite fields.

3.2. Minimal embedding field attacks

Hitt [42] observed that the minimal embedding degree $\mathbb{F}_p^{\mathrm{ord}_N p}$ is not necessarily equal to the field $\mathbb{F}_q^k$, i.e. the extension can be defined over $\mathbb{F}_p$ instead of over $\mathbb{F}_q$. Hence, in this case the group $\mathbf{G}_T$ can be realized as a subgroup of much smaller field yielding to solve the DLP more efficiently in $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_T$. Note that this attack is only applicable for pairing-friendly curves defined over non-prime fields.

3.3. Subgroup attacks

Usually pairing functions are realized in such a way that two out of three groups $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_T$ are proper subgroups of larger composite order subgroups. This results in the so-called subgroup attacks if especially the underlying pairing implementation is not testing the group membership of the elements. Barreto et al. defined the concept of subgroup security and pointed out that most implementations of bilinear maps do not satisfy this notion [10]. They suggested new curve parameters using the known families of pairing-friendly elliptic curves achieving the subgroup security.

4. Hard problems related to pairing

There are plenty of pairing related computational and decisional problems. Their intractabilities form the basic security assumptions upon which pairing-based cryptographic protocols are designed. In this section, we only focus on the most general and frequently used hard problems.

4.1. Pairing inversion problem

A necessary straightforward security assumption is the one-wayness of the underlying pairing function e. The generalized pairing inversion problem (GPInv) asks to find $P \in \mathbf{G}_1$ and $Q \in \mathbf{G}_2$ such that $e(P, Q) = g$ for a given pairing function e and a value $g \in \mathbf{G}_T$. This problem can be divided into two subproblems:

- The fixed argument pairing inversion problem 1 (FAPI-1) is to find $Q \in \mathbf{G}_2$ such that $e(P, Q) = g$ for a given $P \in \mathbf{G}_1$ and $g \in \mathbf{G}_T$.
- The fixed argument pairing inversion problem 2 (FAPI-2) is to find $P \in \mathbf{G}_1$ such that $e(P, Q) = g$ for a given $Q \in \mathbf{G}_2$ and $g \in \mathbf{G}_T$.

A simple observation shows that for each given pair $(P, g) \in \mathbf{G}_1 \times \mathbf{G}_T$ or $(Q, g) \in \mathbf{G}_1 \times \mathbf{G}_T$ both problems FAPI-i, $i = 1, 2,$ have a unique solution by non-degeneracy of e and cyclicity of $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_T$. Note that in the explicit realization of pairings FAPI-i (in terms of the size of the input (P, g) or (Q, g)) can be solved *at most* in subexponential time since there exists a subexponential DLP solver for $\mathbf{G}_T$ (in terms of the input size of $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_T$) by Theorem 1 and discussion in Section 3.1. Again by the discussion in Section 3.1 and Theorem 1 it follows that FAPI-i can even be solved in quasi-polynomial time since there exists a quasi-polynomial DLP solver for $\mathbf{G}_T$ for certain choices of $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_T$. For a detailed relation of the pairing inversion problems and the Diffie–Hellman type assumptions we refer to [34].

Bilinear maps can be computed mainly in two stages. The first one is to compute the evaluation of a certain function at a certain divisor of the underlying elliptic curve E by using Miller's algorithm [11]. The second stage is the *final exponentiation*. For the details about the relationship between the individual steps (Miller inversion and inverting exponentiation) and the pairing inversion problem we also refer to [34].

4.2. Diffie–Hellman related problems

Other most common pairing related problems are as follows:

Definition 1 (Computational bilinear Diffie–Hellman problems [11]). Let e: $\mathbf{G}_1 \times \mathbf{G}_2 \rightarrow \mathbf{G}_T$ be a non-degenerate bilinear pairing. Then

- The bilinear Diffie–Hellman problem 1 (BDH-1) asks to find $e(P, Q)^{ab}$ for given P, aP, $bP \in \mathbf{G}_1$, $Q \in \mathbf{G}_2$ and random a, b.
- The bilinear Diffie–Hellman problem 2 (BDH-2) asks to find $e(P, Q)^{ab}$ for given $P \in \mathbf{G}_1$, aQ, $bQ \in \mathbf{G}_2$ and random elements a, b.

A frequently used variant of the decisional Diffie–Hellman problem in the Type-1 setting ($\mathbf{G}_1 = \mathbf{G}_2$) is given as follows:

Definition 2 (Decisional bilinear Diffie–Hellman problem [11]). Let e: $\mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_T$ with a cyclic group $\mathbf{G}_1 =< P >$ is given. Then

- The decisional bilinear Diffie–Hellman problem (DBDH) is to decide whether $h = e(P, P)^{abc}$ for given P, aP, bP, $cP \in \mathbf{G}_1$ with random elements a, b, c and a random element $h \in \mathbf{G}_T$.

It is clear that the decisional Diffie–Hellman problems including the pairing related ones are solvable in polynomial time when one has oracles solving the computational Diffie–Hellman problems. However, there are groups for which the classical decisional Diffie–Hellman problem is easy while the classical computational Diffie–Hellman problem is believed to be hard. In particular, a gap Dif–Helman group has a distinguishability oracle for which solving the computational problem is hard [16,46]. In the Type-1 pairing setting the Gap Diffie–Hellman Problem is formally defined as follows:

Definition 3 (Gap Diffie–Hellman Problem [16,46]). Given groups $\mathbf{G}_1$ and $\mathbf{G}_2$ of prime order q, a bilinear map e: $\mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_T$ and a generator P of $\mathbf{G}_1$. The Gap Diffie–Hellman Problem (Gap DH) asks to compute abP for given instance (P, aP, bP) of the CDH problem and a DDH oracle.

Since the Gap DH assumption is only realizable with the Type-1 setting, Fact 2 and Definition of the Gap DH assumption implies the following fact:

Fact 4. Protocols using the hardness of the Gap DH assumption should completely be avoided since either

1. the protocols using the Gap DH assumption are insecure if the pairing uses supersingular elliptic curves of small characteristics, or
2. the protocols using the Gap DH assumption are highly inefficient if the pairing uses supersingular elliptic curves of large characteristics.

Definition 4 (Co-assumptions [15]).

- The Computational Co-Diffie–Hellman Problem asks to compute aQ for given P, $aP \in \mathbf{G}_1$ and $Q \in \mathbf{G}_2$ for a random element a.
- The Decisional Co-Diffie–Hellman Problem asks to decide whether $aQ = R$ for given P, $aP \in \mathbf{G}_1$ and Q, $R \in \mathbf{G}_2$, for a random element a.

Assume additionally that $\mathbf{G}_1 \neq \mathbf{G}_2$. Then,

- The Computational Co-Bilinear Diffie–Hellman Problem asks to compute $e(P, Q)^{abc} \in \mathbf{G}_1$ for given $(P, aP, bP) \in \mathbf{G}_1^3$ and $(Q, aQ, cQ) \in \mathbf{G}_2^3$ for random elements a, b and c.

- The Decisional Co-Bilinear Diffie–Hellman Problem asks to distinguish P, aP, bP, Q, $e(P, Q)^{ab}$ from P, aP, bP, Q, $e(P, Q)^{z}$ for random elements a, b and z.

It is trivial to see that the Decisional Co-Diffie–Hellman problem is easy to solve if we have an efficiently computable bilinear map.

The relationship between the CDH and FAPI-1 and FAPI-2 problems is given by the following theorem of Galbraith et al. [34] whose proof follows for a CDH instance (P, aP, bP) easily from first calling the FAPI-1 oracle with the inputs (P, $e(aP, Q)$) to obtain aQ for a random element Q and calling secondly the FAPI-2 oracle (Q, $e(bP, aQ)$):

Theorem 2. *Let e: $\mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$ be a non-degenerate bilinear pairing on cyclic groups of prime order r. Suppose one can solve FAPI-1 and FAPI-2 in polynomial time. Then one can solve the computational Diffie–Hellman problem in $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_T$ in polynomial time.*

Similar to the above argumentation the following result is also proved in [34]:

Theorem 3. *Let notation be as above. If one can solve FAPI-1 (resp. FAPI-2) in polynomial time then one can compute all non-trivial group homomorphisms ϕ_2: $\mathbf{G}_2 \to \mathbf{G}_1$ (resp. ψ_2: $\mathbf{G}_2 \to \mathbf{G}_1$) in polynomial time.*

We continue with an assumption which is frequently used in the design of pairing-based protocols:

Definition 5 (The external Diffie–Hellman (XDH) assumption [13]). Let the CDH be intractable in both $\mathbf{G}_1$ and $\mathbf{G}_2$. The external Diffie–Hellman assumption (XDH) states that the DDH is also intractable in $\mathbf{G}_1$. If the DDH is also intractable in $\mathbf{G}_2$ we have the symmetric external Diffie–Hellman assumption (SXDH).

Remark 2. It is easy to see that the GDH problem is only realizable with the Type-1 pairing, and the strict XDH assumption (i.e. if SXDH does not hold) corresponds exactly to the Type-2 setting. Furthermore, the SXDH assumption is only realizable in the Type-3 setting.

There are also several cryptographic protocols whose security relies on other pairing related problems with auxiliary inputs:

Definition 6 (Pairing problems with auxiliary inputs [24]). Let the elements $g, g^{\alpha}, \ldots, g^{\alpha^d}$ in $\mathbf{G}_1$ (resp. $\mathbf{G}_2$) be given with a random element α. Then, the DLP with auxiliary inputs (DLPwAI) is to compute α. Solving the DLPwAI implies the solution of many pairing-based problem assumptions. These are called pairing problems with auxiliary inputs.

These include the Weak Diffie–Hellman (wDH) Problem, the Strong Diffie–Hellman (sDH) Problem, the Bilinear Diffie–Hellman Inversion (BDHI) Problem and the Bilinear Diffie–Hellman Exponent (BDHE) Problem.

Remark 3. The generalized DLP with auxiliary inputs problem (GDLPwAI) is to compute a randomly chosen α if $g, g^{\alpha^{e_1}}, \ldots, g^{\alpha^{e_d}}$ in $\mathbf{G}_1$ (resp. $\mathbf{G}_2$) are given and $K := \{e_1, \ldots, e_d\}$ is a multiplicatively closed subset of $\mathbb{Z}_{r-1}^{\times}$ [25].

We note that some generalized versions of the Weak Diffie–Hellman (wDH) Problem, the Strong Diffie–Hellman (sDH) Problem, the Bilinear Diffie–Hellman Inversion (BDHI) Problem and the Bilinear Diffie–Hellman Exponent (BDHE) Problem can also be vulnerable if the GDLPwAI is solved.

5. Security or efficiency issues of recent papers

In this section, we revisit a collection of recently proposed research papers in order to illustrate the incorrect use of the pairing-based primitives. We start with a list of recent papers using Type-1 pairings whose underlying schemes can be however easily transformed into the asymmetric settings (Type-2 and Type-3):

1. In [44], the authors propose a batch verification mechanism which aims to verify multiple digital signatures at a time less than the total individual verification time. The authors prove the security of their scheme under the collusion attack assumption in the Type-1 setting with supersingular elliptic curves [44, pp. 2530–2531] which have security issues by Fact 2. Furthermore, the performance analysis is outdated due to the fact that it uses a pairing of embedding degree 3 [44, pp. 2532]. However, the scheme can be easily extended into the Type-3 setting. We note also that this issue still applies most recent papers in cryptography journals such as [43,51,57,70].
2. In [38], the authors propose a privacy-preserving scheme for incentive-based demand response in the smart grid. The smart grid technology basically uses the information and communication technologies aiming to enhance the efficiency, reliability, sustainability of the generation, transmission, distribution, and consumption of electricity. They used a Type-1 pairing [38, pp. 1305] which results in either an insecure or inefficient protocol by Fact 2 even though the scheme only requires the existence of an efficiently computable homomorphism, whence can easily be extended to the Type-2 using the unforgeability of BBS+ signature [13].
3. In [62], the authors propose secure data transmission mechanism for cluster-based wireless sensor networks using the Type-1 setting. Their analysis in [62, pp. 758], however is highly inefficient, i.e. the author's quantitative calculation is much less efficient than transforming the scheme into the Type-3 setting.

4. In [60], a scheme, called TMDP Thin-Model Data Sharing, is proposed to deal with a cloud data sharing scheme utilizing supported keyword search. It also suffers from the use of the Type-1 setting. For instance, the security of the scheme relies on the intractability of the computational Diffie–Hellman problem [60, pp. 125, Lemma 1] which is no longer secure for supersingular elliptic curves over small characteristic finite fields by Fact 2. Hence, the scheme needs to be transformed into the Type-3 setting.
5. The authors in [58] proposed a mechanism using the Type-1 setting for data integrity verification for the Internet of Things (IoT) applications, where the integrity of an outsourced data is the most crucial security property. The authors did not unfortunately modify the original BLS idea into the Type-3 setting which result [58, pp.63] in an insecure or inefficient protocol by Fact 2.
6. In [55], the authors propose an authenticated encryption system using the Type-1 setting aiming to accomplish confidentiality and authenticity simultaneously. This scheme is applied to email system as a practical example. Unfortunately, the proposed example does not have any complexity advantage over the current system. In particular, the scheme is also either insecure or inefficient [55, pp. 631, Theorem 3] because of the use of the Type-1 setting by Fact 2.

The second list gives a collection of papers using Type-1 pairings whose underlying schemes cannot be transformed into the asymmetric setting (since the underlying computational assumptions are only valid for Type-1 pairings) unless the general conversion techniques from Section 2 are used:

1. In [79], the authors present a new Type-1 pairing-based multi-receiver encryption scheme and authenticated key establishment protocol for vehicular ad-hoc network (VANET). Its security analysis relies on the system of [78] which is based on the underlying Gap DH assumption [79, pp. 67, Theorem 2], hence are either insecure or inefficient by Fact 4. Moreover, their example with a 512 bit supersingular elliptic curve with embedding degree 2 is too inefficient since the same security level can be guaranteed in the asymmetric setting for instance with a Barreto–Naehrig (BN) curve [30] of much smaller size.
2. Wang [80] proposes a remote data integrity checking model in multi-cloud platforms. The scheme uses the Gap DH assumption like most of their counterparts (i.e., public auditing schemes) and hence uses the Type-1 setting [80, pp. 336, Lemma 1]. However, the proposed scheme is also either insecure or inefficient by Fact 2. In the simulation of the scheme, the author argued to use 160 bit elliptic curve for the underlying bilinear map [80, pp. 334]. However, we highlight that it is impossible to obtain a secure mechanism using such a small order elliptic curve (either insecure for curves over a field of characteristic 3 or insecure since the embedding degree is 2 over large fields due to the discussions in Section 3.1.).

The third list gives a collection of papers whose underlying schemes use contradictory assumptions and/or timing results:

1. Unlike wired networks, mobile ad-hoc networks (MANETs) are more vulnerable to some attacks bringing new security challenges (e.g., limited resources, open peer-to-peer network, dynamic network topology, lack of a trusted centralized authority). Therefore, designing and implementing more efficient cryptographic protocols, key management, secure neighbor detection, and routing protocol are some of the active research areas. Certificate-less (mostly pairing-based) public key based solutions are known to be one of the best candidates to design such a protocol. But after surveying the pairing-based MANETs, we again realize either an insecure or inefficient use of the Type-1 setting by Fact 2, and counting the pairing operation as a black-box, see for instance [36, pp. 485]. In particular, the simulation results [36, pp. 492–493] use a 160-bit elliptic curve corresponding implicitly to an embedding degree 12 elliptic curve, whence requires the Type-3 setting for example with a BN-curve [30], since otherwise the simulation is totally insecure independent of the field characteristics over which a supersingular elliptic curve in the Type-1 setting is defined.
2. In [27], Coron and Naccache proved that the Co-Diffie Hellmann problem and the k-element aggregate extraction problem are equivalent with the assumption that there exists an efficiently computable homomorphism $\phi: \mathbf{G}_2 \rightarrow \mathbf{G}_1$. Recently, in [83], Xie und Zhang proposed a secure incentive scheme for delay tolerant networks under the k-element aggregate extraction problem using the Type-1 setting. However, it is impossible to convert their scheme into the Type-2 setting. The reason is that their scheme uses the existence of an efficient and secure hashing to point map into $\mathbf{G}_2$, which is in fact not realizable in the Type-2 by Fact 1.
3. Kundu and Bertino [49] propose an authentication mechanism using the Type-1 bilinear maps under the k-element aggregate extraction problem in order to achieve confidentiality-preserving authentication of trees and graphs. As in the above mechanism, an asymmetric modification of the scheme can only be realized in the Type-2 setting since the authors use the original BGLS [15] aggregate signatures. However, this cannot be realized either by Fact 1 because one requires efficient and secure hashing to a point map into $\mathbf{G}_2$.

Remark 4. We note that special attention needs to be given by the design and evaluation of pairing-based protocols in the asymmetric setting, since almost all pairing-based schemes in the literature suffer from the fact that their key sizes, whence timing results, are outdated by Fact 3. Furthermore, we also note that one should completely avoid using pairings with small characteristics in the symmetric setting, since all security and the timing results are invalid, whence outdated, by Facts 1 and 2.

6. Recipe for designers

The following conditions have to be taken into consideration by designing cryptosystems using bilinear maps:

Table 2
Revised version of the comparison of different pairing types [35, Table 1] and the NIST document [66]. A checkmark ✓ denotes that the pairing type satisfies the property and ✗ denotes that it fails to satisfy the property. The # of * measures the efficiency of the underlying pairing type (*** denotes the most efficient choice). Note that p denotes the characteristic of the field over which the curve is defined (i.e. over $\mathbb{F}_q$ with $q = p^n$).

Type	Hash to $\mathbf{G}_2$	Short $\mathbf{G}_1$	Homomorphism	Poly time generation	Security	Efficiency
1 (p=2 or 3)	✓	✗	✓	✗	✗	**
1(large p)	✓	✗	✓	✓	✓	*
2	✗	✓	✓	✓	✓	**
3	✓	✓	✗	✓	✓	***

1. *Use the Type-3 setting*: Although there are automated tools converting protocols using the Type-1 bilinear maps into protocols using the Type-3 bilinear maps [2,4] and a general framework converting the Type-2 schemes into the Type-3 schemes [18], it is always better to design cryptosystems using directly the Type-3 pairing to achieve the best security level and the most efficient protocols. However, one must also be careful about the new complexity bounds on the DLP if the chosen embedding degree is 6 or 12 [48].
2. *Choose the best pairing function*: One should use efficient computation in pairing-friendly groups. In other words, it is crucial to use either optimal pairing [41] or its efficient variants as much as possible. The pairing function should be specified in order to obtain the best efficiency security trade off.
3. *Begin with a correct set-up*: Implementation details should be given more concretely (*what is the desired security level?*) and always together with its usability (*which pairing Type is used?*) and practical aspects (*what is the computation and communication overhead?) and realizability aspects (which pairing function has to be used?*.
4. *Use realizable security assumptions*: It is crucial to avoid unrealizable security assumptions. Furthermore, the assumptions about the security level should be carefully stated using concrete constraints. For a typical example, one may believe that "it is always easy to generate efficiently suitable system parameters for pairing-based cryptosystems" which is clearly wrong as outlined above. See Table 2 for the concrete realizability constraints.
5. *Do not use extensions of binary and ternary curves*: One should be careful about more destructive security issues resulting from attacks on the DLP over fields of small characteristics (following the lines of Section 3.1).
6. *Avoid the explicit homomorphisms*: A possible wrong use of the asymmetric setting with the assumption of the existence of efficiently computable homomorphisms leads to unrealizability and/or security and privacy leakage. We note that in some applications there is a tendency to use the asymmetric setting incorrectly with the assumption of the existence of efficiently computable homomorphisms in both directions (both from $\mathbf{G}_1$ to $\mathbf{G}_2$ and $\mathbf{G}_2$ to $\mathbf{G}_1$). See Table 2 for the concrete realizability constraints.
7. *Use the hashing to point only in the Type-3 setting*: Pairing-based cryptographic protocols may require the following underlying assumptions simultaneously: (1) secure and efficient hashing into group elements (2) efficient homomorphism from $\mathbf{G}_2$ to $\mathbf{G}_1$. This requirement can be vital in order to prove the security of the underlying protocol or to design comparably more efficient mechanisms. However, since both requirements cannot be realized simultaneously in practice, the design criteria should be checked carefully in order to ensure the claimed security and efficiency while achieving a realizable mechanism. See Table 2 for the concrete realizability constraints.
8. *Test group membership or use subgroup secure curves*: In order to undermine the implementation attacks (e.g., failing to test the group membership) subgroup security has to be guaranteed in the realization of pairing-based protocols by generating subgroup secure pairing-friendly elliptic curves following the lines of [10].
9. *Do not use curves over extension fields, use prime fields*: In order to estimate the desired level of security precisely, special caution on the realizability of the minimal embedding field attack has to be taken if the underlying elliptic curves are defined over extension fields. In particular, the equality $\mathrm{ord}_N(p) = mk$ needs to be hold, where $q = p^m$, $\mathbf{G}_1$ is a subgroup of N-th torsion subgroup of the underlying elliptic curve over $\mathbb{F}_q$ and k is the embedding degree.
10. *Take the correct decision on the key sizes*: In order to use composite embedding degrees, the key sizes of the underlying elliptic curves need to be updated by using the complexity results of recent attacks on the medium size finite fields of composite degrees [45,48,72]. For example, possible new pairing-friendly elliptic curves are recently proposed for 128 and 192 bits of security in [8]. The complexity estimates of these new attacks suggest that at most doubling the sizes of the underlying elliptic curves or using elliptic curves of embedding degree one are already safe at the cost of additional computational overhead.
11. *Be careful about the auxiliary inputs*: In order to avoid possible attack scenarios caused by solving the discrete logarithm with auxiliary inputs (DLPwAI) [24] and its generalizations (GDLwAI) [25] special caution has to be taken by the choice of the underlying elliptic curves and the orders of $\mathbf{G}_1$ and $\mathbf{G}_2$. Especially, for the order r of $\mathbf{G}_1$ and $\mathbf{G}_2$ the values $r-1$ and $r+1$ should have no small divisors. Moreover, auxiliary exponents should not be closed with respect to the multiplication. This is important if one needs the security assumptions like the Weak Diffie–Hellman (wDH) Problem, the Strong Diffie–Hellman (sDH) Problem, the Bilinear Diffie–Hellman Inversion (BDHI) Problem and the Bilinear Diffie–Hellman Exponent (BDHE) for the design of the pairing-based protocols.

7. Conclusion

In this paper, we aim to highlight once again the wrong usage of bilinear maps in the recent research papers which unfortunately leads to security, realizability and/or efficiency issues. Furthermore, with the practicality and advantages of pairing-based technologies researchers should focus on the correctness and the mathematical details instead of using them as a "black-box". Moreover, the National Institute of Standards and Technology (NIST) and IEEE have been actively working on the correct versions of pairing-based cryptography to bring them to the state-of-the-art advancements, but the current versions are vulnerable to the recent attacks [1,66].

Acknowledgments

We thank the reviewers for their comments and suggestions which led to improvements in the quality of the paper. Uzunkol's work is supported by the project (114C027) funded by EU FP7-The Marie Curie Action and TÜBİTAK (2236-CO-FUNDED Brain Circulation Scheme). Kiraz's work is supported by a grant from Ministry of Development of Turkey provided to the Cloud Computing and Big Data Research Lab Project.

Appendix. Application areas of pairings

Pairing-based cryptography is being considered for alternative constructions in many areas of cryptographic research. It is an active research area for deploying novel security and privacy mechanisms, e.g., [5,10,19,23,28,31,36,38,44,55,59,68,77,79,84,85]. These include the following applications:

Identity based encryption (IBE) [14]. It is a special type of public-key encryption in which a publicly known identifier is used as a public key. More concretely, a trusted third party first generates its public/private key pair which is called "master" public key and "master" private key. Next, a user's public key is replaced with an identity (e.g., an email, an address, a photo, a phone number, a post address) and his/her private key is computed based on the identity and master private key. IBE allows the user to send an encrypted message to another user using his/her identity as a public key and the user decrypts it with the corresponding public key. IBE based schemes do not require public-key generation and distribution as it exists in the conventional public key systems, which significantly reduce/eliminate the cost and complexity of generating and managing users' certificates (i.e., a public key infrastructure). It has further an interesting property that private keys need not to be generated before sending an encrypted message.

Hierarchical identity-based encryption (HIBE) [12]. It allows the private key generator to delegate its computation to the lower-level private key generators. Furthermore, anonymous HIBE is an extension of IBE which hides not only the message itself but also the identity of the users. Anonymous HIBE solutions can be applied to anonymous communication systems and public key encryption systems with a keyword searching mechanism.

Functional (or attribute based) encryption [52,53]. It uses pairings to generate decryption keys which allows a user possessing an encrypted data $\mathsf{Enc}(x)$ to compute $f(x)$ of the data for an arbitrary function f.

IBE with threshold decryption [7]. The master key of the trusted third party of a standard IBE system can be distributed in a (k, n) fashion among n different independent authorities, where at least k of them must cooperate and collude to perform decryption (using conventional techniques of threshold cryptography like Shamir secret sharing schemes).

Searchable encryption [29]. It allows a user to compute whether a given keyword exists in an encrypted message without giving away any information about the message itself. In practice, it is possible to search any query on an encrypted database without decryption (e.g., patient medical records, biometric data, personal data, corporate data, intellectual property).

Signatures [11,75]. Digital signatures is an important primitive which ensures authentication, integrity of a message, and non-repudiation. Apart from conventional signature schemes (based on RSA or ECC) pairing/ID based signatures are constructed because of some nice structural properties like homomorphic linear authenticators where the authenticators can be aggregated into only one tag, which significantly reduces the communication and computational complexity. Other types of pairing-based signature schemes include short signatures (also without random oracles), blind signatures (where a user obtains a signature from a signer while the signer does not learn any information about the message being signed), identity based signatures (also including ID-based blind signatures, hierarchical ID-based signatures, ring signatures), chameleon signatures (non-repudiable and non-transferrable), aggregate signatures (which allows multiple signatures to be aggregated into one compact signature), ring signatures (where any group member can sign a message without learning any information about the signed message), group signatures (which is similar to ring signatures except that a "group manager" can detect which group member indeed signed a message), threshold signatures (a valid signature can be computed only if at least t signers cooperate), authentication-tree based signatures without random oracles.

New security requirements for cloud and IoT security. Privacy enhancing techniques (like privacy-preserving auctions, anonymous credentials, or privacy-friendly aggregation for the smart grid), proofs of retrievability of data for cloud storage systems [75], internet of things (IoT) [54], e-health systems and wearable technologies [61].

Other applications. Last but not least, there are also various ID based mechanisms including authentication [17,56], identity based key-agreement [22,81], signcryption (which is a public key authenticated encryption, i.e. including both signing and encrypting operations simultaneously), and identity based Chameleon hashes [6] (which are collision resistant functions with a trapdoor for finding collisions).

References

[1] IEEE standard for identity-based cryptographic techniques using pairings, IEEE Std 1363.3-2013 (2013) 1–151, doi:10.1109/IEEESTD.2013.6662370.

[2] M. Abe, J. Groth, M. Ohkubo, T. Tango, Converting cryptographic schemes from symmetric to asymmetric bilinear groups, in: Proceedings of the Advances in Cryptology CRYPTO 2014, in: Lecture Notes in Computer Science, 8616, Springer Berlin Heidelberg, 2014, pp. 241–260.

[3] G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez, Computing discrete logarithms in $\mathbb{F}_3^6 \cdot 137$ and $\mathbb{F}_3^6 \cdot 163$ using magma, in: C.K. Koç, S. Mesnager, E. Savaş (Eds.), Arithmetic of Finite Fields, Springer International Publishing, Cham, 2015, pp. 3–22.

[4] J.A. Akinyele, C. Garman, S. Hohenberger, Automating fast and secure translations from type-i to type-iii pairing schemes, in: Proceedings of the Twenty-second ACM SIGSAC Conference on Computer and Communications Security, CCS '15, ACM, 2015, pp. 1370–1381.

[5] T. Asami, B. Namsraijav, Y. Kawahara, K. Sugiyama, A. Tagami, T. Yagyu, K. Nakamura, T. Hasegawa, Moderator-controlled information sharing by identity-based aggregate signatures for information centric networking, in: Proceedings of the Second International Conference on Information-Centric Networking, ICN '15, ACM, 2015, pp. 157–166.

[6] G. Ateniese, B. Medeiros, Proceedings of the Financial Cryptography: Eighth International Conference, FC 2004, Key West, FL, USA, Springer Berlin Heidelberg, Berlin, Heidelberg, February 9-12, 2004, pp. 164–180. Revised Papers, 10.1007/978-3-540-27809-2_19.

[7] J. Baek, Y. Zheng, Identity-based threshold decryption, in: Proceedings of the Seventh International Workshop on Theory and Practice in Public Key Cryptography (PKC), in: Lecture Notes in Computer Science, LCNS 2047, Springer Berlin Heidelberg, 2004, pp. 262–276.

[8] R. Barbulescu, S. Duquesne, Updating key size estimations for pairings, J. Cryptol. (2018), doi:10.1007/s00145-018-9280-5.

[9] R. Barbulescu, P. Gaudry, A. Joux, E. Thomé, Proceedings of the Advances in Cryptology – EUROCRYPT 2014: Thirty-third Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 1–16.

[10] P. Barreto, C. Costello, R. Misoczki, M. Naehrig, G. Pereira, G. Zanon, Subgroup security in pairing-based cryptography, in: Proceedings of the Progress in Cryptology – LATINCRYPT 2015, in: Lecture Notes in Computer Science, 9230, Springer International Publishing, 2015, pp. 245–265.

[11] I. Blake, G. Seroussi, N. Smart, Advances in Elliptic Curve Cryptography, London Mathematical Society Lecture Note Series, Cambridge University Press, New York, NY, USA, 2005.

[12] D. Boneh, X. Boyen, E.-J. Goh, Proceedings of the Advances in Cryptology – EUROCRYPT 2005: Twenty-forth Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, Berlin, Heidelberg, May 22-26, 2005, pp. 440–456. Aarhus, Denmark.

[13] D. Boneh, X. Boyen, H. Shacham, Proceedings of the Advances in Cryptology – CRYPTO 2004: Twenty-forth Annual International Cryptology Conference, Springer Berlin Heidelberg, Berlin, Heidelberg, August 15-19, 2004, pp. 41–55. Santa Barbara, California, USA.

[14] D. Boneh, M. Franklin, Identity-Based Encryption from the Weil Pairing, Springer Berlin Heidelberg, Berlin, Heidelberg, 2001, pp. 213–229.

[15] D. Boneh, C. Gentry, B. Lynn, H. Shacham, Proceedings of the Advances in Cryptology – EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, Berlin, Heidelberg, May 4-8, 2003, pp. 416–432. Warsaw, Poland.

[16] D. Boneh, B. Lynn, H. Shacham, Short signatures from the weil pairing, in: Proceedings of the Advances in Cryptology, ASIACRYPT 2001, in: Lecture Notes in Computer Science, 224, Springer Berlin Heidelberg, 2001, pp. 514–532.

[17] V. Cakulev, G. Sundaram, MIKEY-IBAKE: Identity-Based Authenticated Key Exchange (IBAKE) Mode of Key Distribution in Multimedia Internet KEYing (MIKEY), 2011, (RFC 6267), doi:https://doi.org/10.17487/RFC6267.

[18] S. Chatterjee, A. Menezes, On cryptographic protocols employing asymmetric pairings – the role of ψ revisited, Discr. Appl. Math. 159 (13) (2011) 1311–1322, doi:10.1016/j.dam.2011.04.021.

[19] S. Chatterjee, A. Menezes, Type 2 structure-preserving signature schemes revisited, in: Proceedings of the Advances in Cryptology ASIACRYPT 2015, in: Lecture Notes in Computer Science, 9452, Springer Berlin Heidelberg, 2015, pp. 286–310.

[20] S. Chatterjee, A. Menezes, F. Rodriguez-Henriquez, On instantiating pairing-based protocols with elliptic curves of embedding degree one, IEEE Trans. Comput. 66 (6) (2017) 1061–1070.

[21] J. Chen, H.W. Lim, S. Ling, H. Wang, H. Wee, Proceedings of the Pairing-Based Cryptography – Pairing 2012: Fifth International Conference, Springer Berlin Heidelberg, Berlin, Heidelberg, May 16-18, 2012, pp. 122–140. Cologne, Germany, Revised Selected Papers.

[22] L. Chen, Z. Cheng, N.P. Smart, Identity-based key agreement protocols from pairings, Int. J. Inf. Secur. 6 (4) (2007) 213–241, doi:10.1007/s10207-006-0011-9.

[23] P. Chen, X. Wang, J. Su, A hierarchical identity-based signature from composite order bilinear groups, in: Proceedings of the Algorithms and Architectures for Parallel Processing, in: Lecture Notes in Computer Science, 9532, Springer International Publishing, 2015, pp. 46–56.

[24] J.H. Cheon, T. Kim, A new approach to the discrete logarithm problem with auxiliary inputs, LMS J. Comput. Math. 19 (1) (2016) 1–15.

[25] J.H. Cheon, T. Kim, Y.S. Song, Proceedings of the Twentieth International Conference Selected Areas in Cryptography – SAC 2013, Springer Berlin Heidelberg, Berlin, Heidelberg, August 14-16, 2013, pp. 121–135. Burnaby, BC, Canada, Revised Selected Papers.

[26] , Handbook of Elliptic and Hyperelliptic Curve Cryptography, in: H. Cohen, G. Frey (Eds.), CRC Press, 2005.

[27] J.-S. Coron, D. Naccache, Proceedings of the Advances in Cryptology – ASIACRYPT 2003: Ninth International Conference on the Theory and Application of Cryptology and Information Security, Springer Berlin Heidelberg, November 30-December 4, 2003, pp. 392–397. Taipei, Taiwan.

[28] A. Enge, J. Milan, Implementing Cryptographic Pairings at Standard Security Levels, in: Lecture Notes in Computer Science, 8804, Springer International Publishing, 2014, pp. 28–46.

[29] L. Fang, W. Susilo, C. Ge, J. Wang, Public key encryption with keyword search secure against keyword guessing attacks without random oracle, Inf. Sci. 238 (2013) 221–241.

[30] D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves, J. Cryptol. 23 (2) (2010) 224–280, doi:10.1007/s00145-009-9048-z.

[31] E.S.V. Freire, Non-interactive key exchange and key assignment schemes, Stanford University, 2014 Phd Thesis.

[32] G. Frey, H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Math. Comput. 62 (206) (1994) 865–874, doi:10.2307/2153546.

[33] S.D. Galbraith, P. Gaudry, Recent progress on the elliptic curve discrete logarithm problem, Des. Codes Cryptogr. 78 (1) (2015) 51–72.

[34] S.D. Galbraith, F. Hess, F. Vercauteren, Aspects of pairing inversion, IEEE Trans. Inf. Theory 54 (12) (2008) 5719–5728.

[35] S.D. Galbraith, K.G. Paterson, N.P. Smart, Pairings for cryptographers, Discr. Appl. Math. 156 (16) (2008) 3113–3121.

[36] U. Ghosh, R. Datta, A secure addressing scheme for large-scale managed manets, IEEE Trans. Netw. Serv. Manag. 12 (3) (2015) 483–495.

[37] F. Göloğlu, R. Granger, G. McGuire, J. Zumbrägel, On the Function Field Sieve and the Impact of Higher Splitting Probabilities, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 109–128.

[38] Y. Gong, Y. Cai, Y. Guo, Y. Fang, A privacy-preserving scheme for incentive-based demand response in the smart grid, IEEE Trans. Smart Grid (99) (2015), doi:10.1109/TSG.2015.2412091.

[39] R. Granger, T. Kleinjung, J. Zumbrägel, '128-bit Secure' Supersingular Binary Curves, in: Advances in Cryptology - CRYPTO 2014, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 126–145.

[40] R. Granger, T. Kleinjung, J. Zumbrägel, On the discrete logarithm problem in finite fields of fixed characteristic, IACR Cryptology ePrint Archive, vol. 2015, 2015, p. 685.

[41] F. Hess, Pairing lattices, in: S. Galbraith, K. Paterson (Eds.), Proceedings of the Pairing-Based Cryptography Pairing 2008, Lecture Notes in Computer Science, 5209, Springer Berlin Heidelberg, 2008, pp. 18–38, doi:10.1007/978-3-540-85538-5_2.

[42] L. Hitt, Proceedings of the Pairing-Based Cryptography – Pairing 2007: First International Conference, Springer Berlin Heidelberg, July 2-4, 2007, pp. 294–301. Tokyo, Japan.

[43] D. Hofheinz, T. Jager, Tightly secure signatures and public-key encryption, Des. Codes Cryptogr. 80 (1) (2015) 29–61.

[44] J.Y. Hwang, D.H. Choi, H. Cho, B. Song, New efficient batch verification for an identity-based signature scheme, Secur. Communication Networks 8 (15) (2015) 2524–2535.

[45] T. Kim, J. Jeong, Extended tower number field sieve with application to finite fields of arbitrary composite extension degree, in: S. Fehr (Ed.), Public-Key Cryptography – PKC 2017, Springer Berlin Heidelberg, Berlin, Heidelberg, 2017, pp. 388–408.

[46] A. Joux, K. Nguyen, Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups, J. Cryptol. 16 (4) (2003) 239–247.

[47] A. Joux, C. Pierrot, Technical history of discrete logarithms in small characteristic finite fields, Des. Codes Cryptogr. 78 (1) (2016) 73–85, doi:10.1007/s10623-015-0147-6.

[48] T. Kim, R. Barbulescu, Proceedings of the Advances in Cryptology – CRYPTO 2016: Thirty-second Annual Cryptology Conference, Springer Berlin Heidelberg, Berlin, Heidelberg, August 14-18, 2012. Santa Barbara, CA, USA.

[49] A. Kundu, E. Bertino, Privacy-preserving authentication of trees and graphs, Int. J. Inf. Secur. 12 (6) (2013) 467–494.

[50] N.P.S. L. Chen Z. Cheng, Identity-based key agreement protocols from pairings, Int. J. Inf. Secur. 6 (4) (2007) 213–241, doi:10.1007/s10207-006-0011-9.

[51] K. Lee, Self-updatable encryption with short public parameters and its extensions, Des. Codes Cryptogr. 79 (1) (2016) 121–161.

[52] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, Proceedings of the Advances in Cryptology – EUROCRYPT 2010: Twenty-Ninth Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, Berlin, Heidelberg, May 30-June 3, 2010, pp. 62–91. French Riviera.

[53] A. Lewko, B. Waters, Proceedings of the Advances in Cryptology – EUROCRYPT 2011: Thirtieth Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, Springer Berlin Heidelberg, Berlin, Heidelberg, May 15-19, 2011, pp. 568–588. 10.1007/978-3-642-20465-4_31.

[54] F. Li, P. Xiong, Practical secure communication for integrating wireless sensor networks into the internet of things, IEEE Sens. J. 13 (10) (2013) 3677–3684.

[55] F. Li, Z. Zheng, C. Jin, Identity-based deniable authenticated encryption and its application to e-mail system, Telecommun. Syst. (2015) 1–15.

[56] H. Li, Y. Dai, L. Tian, H. Yang, Proceedings of the Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, Springer Berlin Heidelberg, Berlin, Heidelberg, December 1-4, 2009, pp. 157–166. 10.1007/978-3-642-10665-1_14.

[57] B. Libert, T. Peters, M. Joye, M. Yung, Linearly homomorphic structure-preserving signatures and their applications, Des. Codes Cryptogr. 77 (2) (2015) 441–477.

[58] C. Liu, C. Yang, X. Zhang, J. Chen, External integrity verification for outsourced big data in cloud and IOt, Future Gener. Comput. Syst. 49 (C) (2015) 58–67, doi:10.1016/j.future.2014.08.007.

[59] J. Liu, Z. Zhang, X. Chen, K.S. Kwak, Certificateless remote anonymous authentication schemes for wirelessbody area networks, IEEE Trans. Paral. Distrib. Syst. 25 (2) (2014) 332–342.

[60] Z. Liu, J. Li, X. Chen, J. Yang, C. Jia, Proceedings of the Information Security and Privacy: Ninteenth Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, Springer International Publishing, Cham, July 7-9, 2014, pp. 115–130. 10.1007/978-3-319-08344-5_8.

[61] A. Lounis, A. Hadjidj, A. Bouabdallah, Y. Challal, Secure and scalable cloud-based architecture for e-health wireless sensor networks, in: Proceedings of the 2012 Twenty-first International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1–7.

[62] H. Lu, J. Li, M. Guizani, Secure and efficient data transmission for cluster-based wireless sensor networks, IEEE Trans. Paral. Distrib. Syst. 25 (3) (2014) 750–761.

[63] F. Luca, D.J. Mireles, I.E. Shparlinski, Mov attack in various subgroups on elliptic curves, Illin. J. Math. 48 (3) (2004) 1041–1052.

[64] M. Massierer, Some experiments investigating a possible L(1/4) algorithm for the discrete logarithm problem in algebraic curves, IACR Cryptol. ePrint Archive 2014 (2014) 996.

[65] A. Menezes, T. Okamoto, S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Trans. Inf. Theory 39 (5) (1993) 1639–1646, doi:10.1109/18.259647.

[66] D. Moody, R. Peralta, R. Perlner, A. Regenscheid, A. Roginsky, L. Chen, in: J. Res. Natl. Inst. Stand. Technol., 120, 2015, pp. 11–27. https://doi.org/10.6028/jres.120.002.

[67] N.E. Mrabet, N. Guillermin, S. Ionica, A study of pairing computation for elliptic curves with embedding degree 15, IACR Cryptol. ePrint Archive 2009 (2009) 370.

[68] L. Nkenyereye, K. Rhee, Secure traffic data transmission protocol for vehicular cloud, in: Proceedings of the Advances in Computer Science and Ubiquitous Computing, in: Lecture Notes in Electrical Engineering, 373, Springer Singapore, 2015, pp. 497–503.

[69] A.M. Odlyzko, Advances in Cryptology: Proceedings of EUROCRYPT 84 A Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, Springer Berlin Heidelberg, Berlin, Heidelberg, April 9-11, 1984, pp. 224–314.

[70] T. Okamoto, K. Takashima, Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption, Des. Codes Cryptogr. 77 (2) (2015) 725–771.

[71] S.C. Ramanna, S. Chatterjee, P. Sarkar, Proceedings o the Public Key Cryptography – PKC 2012: Fifteenth International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, Proceedings, Springer Berlin Heidelberg, Berlin, Heidelberg, May 21-23, 2012, pp. 298–315. 10.1007/978-3-642-30057-8_18.

[72] P. Sarkar, S. Singh, A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm, Advances in Cryptology — ASIACRYPT 2016, Springer, Berlin Heidelberg, 2016.

[73] I. Semaev, New algorithm for the discrete logarithm problem on elliptic curves, IACR Cryptology ePrint Archive (2015).

[74] H. Shacham, New Paradigms in Signature Schemes, Stanford, CA, USA, 2006 Ph.D. thesis.

[75] H. Shacham, B. Waters, Compact proofs of retrievability, in: Proceedings of theAdvances in Cryptology – ASIACRYPT 2008, in: Lecture Notes in Computer Science, 5350, Springer Berlin Heidelberg, 2008, pp. 90–107.

[76] V. Shoup, Advances in Cryptology — EUROCRYPT '97: International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 256–266.

[77] J. Tsai, A new efficient certificateless short signature scheme using bilinear pairings, IEEE Syst. J. PP (99) (2015) 1–8.

[78] Y.-M. Tseng, Y.-H. Huang, H.-J. Chang, Cca-secure anonymous multi-receiver id-based encryption, in: Proceedings of the 2012 Twenty-sixth International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2012, pp. 177–182.

[79] C. Wang, D. Shi, X. Xu, J. Fang, An anonymous data access scheme for vanet using pseudonym-based cryptography, J. Ambient Intell. Hum. Comput. (2015) 1–9.

[80] H. Wang, Identity-based distributed provable data possession in multicloud storage, IEEE Trans. Serv. Comput. 8 (2) (2015) 328–340.

[81] Y. Wang, Transactions on Computational Science XVII, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 172–197. 10.1007/978-3-642-35840-1_9

[82] B. Waters, Proceedings of the Advances in Cryptology – CRYPTO 2009: Twenty-ninth Annual International Cryptology Conference, Springer Berlin Heidelberg, August 16-20, 2009, pp. 619–636. Santa Barbara, CA, USA.
[83] Y. Xie, Y. Zhang, A secure, service priority-based incentive scheme for delay tolerant networks, Secur. Commun. Netw. 9 (1) (2016) 5–18.
[84] P. Xu, Q. Wu, W. Wang, W. Susilo, J. Domingo-Ferrer, H. Jin, Generating searchable public-key ciphertexts with hidden structures for fast keyword search, IEEE Trans. Inf. Forens. Secur. 10 (9) (2015) 1993–2006.
[85] E. Zavattoni, L. Dominguez Perez, S. Mitsunari, A. Sanchez-Ramrez, T. Teruya, F. Rodriguez-Henriquez, Software implementation of an attribute-based encryption scheme, IEEE Tran. Comput. 64 (5) (2015) 1429–1441.