Still Wrong Use of Pairings in Cryptography

Mehmet Sabır Kiraz and Osmanbey Uzunkol
Mathematical and Computational Sciences Labs
TÜBİTAK BİLGEM, Turkey
{mehmet.kiraz,osmanbey.uzunkol}@tubitak.gov.tr

Abstract. Several pairing-based cryptographic protocols are recently proposed with a wide variety of new novel applications including the ones in 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. The paper of Galbraith, Paterson, and Smart (2006) pointed out most of the issues related to the incorrect use of pairing-based cryptography. However, we noticed that some recently proposed applications still do not use these primitives correctly. This leads to unrealizable, insecure or too inefficient designs of pairing-based protocols. We observed that one reason is not being aware of the recent advancements on solving the discrete logarithm problems in some groups. The main purpose of this article is to give an understandable, informative, and the most up-to-date criteria for the correct use of pairing-based cryptography. We thereby deliberately avoid most of the technical details and rather give special emphasis on the importance of the correct use of bilinear maps by realizing secure cryptographic protocols. We list a collection of some recent papers having wrong security assumptions or realizability/efficiency issues. Finally, we give a compact and an up-to-date recipe of the correct use of pairings.

Keywords: Pairing-Based Protocols, Bilinear Maps, Security, Efficiency, The Discrete Logarithm Problem.

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 7 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 [64].

There have been unfortunately a collection of results using the pairing-based primitives incorrectly. In fact, Galbraith, Paterson, and Smart drew attention to the potential problems related to using these "black boxes" incorrectly [34]. However, we notice that many recent research papers still have security vulnerabilities, realizability issues and/or efficiency problems since the appearance of [34]. These papers (surprisingly) either have pairing related wrong security assumptions regarding the infeasibility of certain computational problems and/or efficiency issues. The main reason is to use pairing-based primitives as "black-boxes" without giving attention on the concrete realizations of these primitives.

The security of pairing-based cryptosystems relies on the difficulty of various computationally hard problems related to the discrete logarithm problem (DLP). However, there are also new attacks on the DLP on some groups [3,8,36,38,67]. These attacks have major consequences on the design of secure cryptographic protocols based on pairing-based cryptography. Hence, one additional relatively new reason of incorrect use of pairing-based primitives is to ignore these recent technical advancements in solving the DLP which make certain security assumptions incorrect. The complexity of these mathematical preliminaries is undoubtedly the reason of neglecting the realization concerns in the design of pairing-based protocols. Furthermore, Kim and Barbulescu [46] reduces the complexity of the DLP for medium size primes very recently which have certain consequences on some other pairing primitives.

In this work, our aim is to highlight the importance of correct choices and their affect on the realizability of abstract pairing requirements to design cryptographic protocols with prescribed level of security, realizability and desired efficiency. In this respect, we briefly survey the most recent attacks against pairing-based cryptography which have direct effects on the designs and the security models of cryptographic protocols. We further emphasize the concerns in the paper of Galbraith, Paterson, and Smart [34] together with further new security issues and their implications. We stress thereby that this paper does not propose new improvements or new mathematical techniques but deliberately give attention to the incorrect use of pairings. Therefore, our purpose is to give an informative and less technical overview of pairing-based mechanisms which briefly surveys the various pairing-based real-world applications while taking the recent mathematical improvements having direct security and efficiency implications into account. Furthermore, we give a more detailed list on various pairing related hard problems together with their relation to the security assumptions of the underlying pairing-based protocols. We fi-

nally propose a compact and state-of-the-art recipe for designers to take it into consideration for proper usage. This recipe covers main security and realizability issues of pairing-based cryptography which may help the designers to use the primitives correctly.

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 [34, 71] 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 $\phi : \mathbf{G}_2 \to \mathbf{G}_1$. 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 $\phi : \mathbf{G}_2 \to \mathbf{G}_1$.

– **Type-4:** $\mathbf{G}_1 \neq \mathbf{G}_2$ and there exists an efficiently computable homomorphism $\phi : \mathbf{G}_2 \to \mathbf{G}_1$ as in the case of the Type-2 setting but with an efficient secure hashing method to a group element [71]. Security proofs can be quite cumbersome in this setting as discussed in [48]. 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 $\mathbf{G}_2$, [34, 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 [17, Section 5].

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) [10].

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 [19, 69, 79]. 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 [19, 69, 79]. 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 $Q \stackrel{?}{=} abP$ 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. *[31, 63] 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 [31, 63].

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 [3,8,36,38,67]. 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, 38]. Concrete attacks are performed for certain supersingular elliptic/hyperelliptic curves over $\mathbb{F}_2$ and $\mathbb{F}_3$, see [3,38]. Difficulties of generalizing these attacks on the elliptic curve setting are pointed out in a recent work of Massierer [62]. 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 [70] 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 [32].

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

3.1 Quasi-polynomial Attacks on the DLP and Bilinear Maps

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 order of $\mathbf{G}$ [73]. In particular, computing the discrete logarithms in generic groups requires approximately $\sqrt{p}$ computation in $\mathbf{G}$.

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 has 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 Joux et al. [8] and Göloglu et al. [36]. Recently, Granger et al. [39] improved the result of Joux et al. [8] 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.

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 [45]. In fact, subsequent results applying the idea of this algorithm (combined with Frey-Rück and MOV attacks [25]) showed the fatal security issues for cryptographic protocols using the Type-1 bilinear maps [3, 8, 38, 67].

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. [8] 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.

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 [10] 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 [40]. 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 [29] for the details. For implementation and comparison purposes, one can consult Table 1 following the lines of [65].

The probability that a randomly chosen (nearly) prime order elliptic curve E has small enough embedding degree is negligibly small (generically k is in $O(q)$) [29, 61]. Hence, special pairing-friendly curves have to be constructed in order to realize an efficiently computable function e

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 $q \mod r$) [65].

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	12480 MM
192	384	7000-9000	18-24	17007 MM	31200 MM
256	512	14000-18000	28-36	33486 MM	62400 MM

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 $\text{char}(\mathbb{F}_q) \neq 2, 3, \text{char}(\mathbb{F}_q) = 2$ and $\text{char}(\mathbb{F}_q) = 3$, respectively [10]. We refer to [29] 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).

Consequences of the Attack 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, 8, 36, 38, 67]. Since the Type-1 pairing can only be realized using supersingular elliptic/hyperelliptic curves [34] we see in Section 4 that all Type-1 bilinear maps and the related protocols are either useless or regarded completely as insecure.

3.2 Minimal Embedding Field Attacks

Hitt [41] observed that the minimal embedding degree $\mathbb{F}_p^{\mathrm{ord}_{Np}}$ 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 [9]. 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 [33].

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 [10]. 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 [33].

4.2 Diffie-Hellman Related Problems

Other most common pairing related problems are as follows:

Definition 1 (Computational Bilinear Diffie-Hellman Problems [10]).
Let $e : \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$ 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 [10]).
Let $e : \mathbf{G}_1 \times \mathbf{G}_1 \to \mathbf{G}_T$ 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 Diffi-Helman group has a distinguishability oracle for which solving the computational problem is hard [15, 44]. In the Type-1 pairing setting the Gap Diffie-Hellman Problem is formally defined as follows:

Definition 3 (Gap Diffie-Hellman Problem [15,44]). *Given groups* $\mathbf{G}_1$ *and* $\mathbf{G}_2$ *of prime order* q*, a bilinear map* $e : \mathbf{G}_1 \times \mathbf{G}_1 \to \mathbf{G}_T$ *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.*

Definition 4 (Co-Assumptions [14]).

- *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. [33] 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 [33]:

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* $\phi_2 : \mathbf{G}_2 \to \mathbf{G}_1$ *(resp.* $\psi_2 : \mathbf{G}_2 \to \mathbf{G}_1$*) 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 [12]). *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 1. 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 [22]). *Let the elements* $g, g^{\alpha}, \cdots, g^{\alpha^d}$ *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 2. The generalized DLP with auxiliary inputs problem (GDLPwAI) is to compute a randomly chosen α if $g, g^{\alpha^{e_1}}, \cdots, g^{\alpha^{e_d}}$ in $\mathbf{G}_1$ (resp. $\mathbf{G}_2$) are given and $K := \{e_1, \cdots, e_d\}$ is a multiplicatively closed subset of $\mathbb{Z}_{r-1}^{\times}$ [23].

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.

- In [43], 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 using the Type-1 setting with supersingular elliptic curves [43, pp.2526] having security issues as discussed in Section 3.1. We note also that this issue still applies most recent papers in cryptography journals such as [42, 49, 55, 68].
- In [76], 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 [75] which is based on the underlying Gap DH, hence realizable only in the Type-1 setting. 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 curve of 160 bits [29].
- In [53], the authors proposed 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. The scheme is also too inefficient because of the use of the Type-1 setting as in the previously mentioned schemes.
- In [37] 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 although the security of the scheme relies on the existence of an efficiently computable homomorphism in the Type-2 setting as stated in [37] using the unforgeability of BBS+ signature [12]. Therefore, the scheme has to be modified into a more efficient Type-3 setting in the light of [17].
- 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 algorithms, 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. But after surveying the pairing-based MANETs, we again realize the incorrect use of the Type-1 setting and counting the pairing operation as a black-box, see for instance [35].

- In [24], the authors proposed a solution for scalable data sharing in cloud storage using key-aggregate cryptosystems using the Type-1 setting. A subsequent paper [58] deals with a cloud data sharing scheme utilizing supported keyword search. It also suffers from the use of the Type-1 setting. For instance, in the latter paper, the security of the scheme relies on the intractability of the computational Diffie-Hellman problem which is no longer secure for supersingular elliptic curves over small characteristic finite fields as discussed in Section 3.1.
- The authors in [56] 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.
- In [60] the authors proposed secure data transmission mechanism for cluster-based wireless sensor networks using the Type-1 setting. Their analysis in [60, pp. 758], however, cannot be realized in this setting. Therefore, the proposed scheme is much less efficient than the author's quantitative calculation.
- The author proposes in [77] a remote data integrity checking model in multi-cloud platforms. The scheme uses the Gap DH assumptions like most of their counterparts (public auditing schemes) and hence uses the Type-1 setting. In the simulation of the scheme the author argued to use 160 bit elliptic curve for the underlying bilinear map. 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.)
- In [26], 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 [80] 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 setting as discussed in Section 2.
– Kundu and Bertino [47] proposed 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 author uses the original BGLS [14] aggregate signatures. However, this cannot be realized either, since one requires efficient and secure hashing to a point map into $\mathbf{G}_2$.

6 Recipe for Designers

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

– **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 [17], 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 [46].
– **Choose the Best Pairing Function:** One should use efficient computation in pairing-friendly groups. In other words use optimal pairing [40] or its efficient variants as much as possible. The pairing function should be specified in order to obtain the best efficiency security trade off.
– **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?*.
– **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.

Table 2. Revised version of the comparison of different pairing types [34, Table 1]. 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	✓	✓	✗	✓	✓	***

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 1 for the concrete realizability constraints.

– **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).

– **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 1 for the concrete realizability constraints.

– **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 1 for the concrete realizability constraints.
- **Test Group Membership or Use Subgroup Secure Curves:** In order to undermine the implementation attacks (for instance, 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 [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.
- **Be Careful about the Auxiliary Inputs:** In order to avoid possible attack scenarios caused by solving the discrete logarithm with auxiliary inputs (DLPwAI) [22] and its generalizations (GDLwAI) [23] 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, 64].

Acknowledgements

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. 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).

References

1. IEEE standard for identity-based cryptographic techniques using pairings. *IEEE Std 1363.3-2013*, pages 1–151, Nov 2013.
2. M. Abe, J. Groth, M. Ohkubo, and T. Tango. Converting cryptographic schemes from symmetric to asymmetric bilinear groups. In *Advances in Cryptology CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 241–260. Springer Berlin Heidelberg, 2014.
3. G. Adj, A. Menezes, T. Oliveira, and F. Rodríguez-Henríquez. Computing discrete logarithms in $\mathbb{F}_{3^{6\cdot 137}}$ using magma. *IACR Cryptology ePrint Archive*, 2014:57, 2014.
4. J. A. Akinyele, C. Garman, and S. Hohenberger. Automating fast and secure translations from type-i to type-iii pairing schemes. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 1370–1381. ACM, 2015.
5. T. Asami, B. Namsraijav, Y. Kawahara, K. Sugiyama, A. Tagami, T. Yagyu, K. Nakamura, and T. Hasegawa. Moderator-controlled information sharing by identity-based aggregate signatures for information centric networking. In *Proceedings of the 2nd International Conference on Information-Centric Networking*, ICN '15, pages 157–166. ACM, 2015.
6. G. Ateniese and B. Medeiros. *Financial Cryptography: 8th International Conference, FC 2004, Key West, FL, USA, February 9-12, 2004. Revised Papers*, chapter Identity-Based Chameleon Hash and Applications, pages 164–180. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.
7. J. Baek and Y. Zheng. Identity-based threshold decryption. In *7th International Workshop on Theory and Practice in Public Key Cryptography (PKC)*, volume 2047, pages 262–276. Springer Berlin Heidelberg - Lecture Notes in Computer Science, 2004.
8. R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. *Advances in Cryptology – EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, chapter A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic, pages 1–16. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
9. P. Barreto, C. Costello, R. Misoczki, M. Naehrig, G. Pereira, and G. Zanon. Subgroup security in pairing-based cryptography. In *Progress in Cryptology – LATINCRYPT 2015*, volume 9230 of *Lecture Notes in Computer Science*, pages 245–265. Springer International Publishing, 2015.

10. I. Blake, G. Seroussi, and N. Smart. *Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series)*. Cambridge University Press, New York, NY, USA, 2005.
11. D. Boneh, X. Boyen, and E.-J. Goh. *Advances in Cryptology – EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings*, chapter Hierarchical Identity Based Encryption with Constant Size Ciphertext, pages 440–456. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.
12. D. Boneh, X. Boyen, and H. Shacham. *Advances in Cryptology – CRYPTO 2004: 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004. Proceedings*, chapter Short Group Signatures, pages 41–55. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.
13. D. Boneh and M. Franklin. *Identity-Based Encryption from the Weil Pairing*, pages 213–229. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001.
14. D. Boneh, C. Gentry, B. Lynn, and H. Shacham. *Advances in Cryptology — EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings*, chapter Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, pages 416–432. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.
15. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. In *Advances in Cryptology, ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer Berlin Heidelberg, 2001.
16. V. Cakulev, G. Sundaram, and I. Broustis. *IBAKE: Identity-Based Authenticated Key Exchange*. RFC 6539, 2012.
17. S. Chatterjee and A. Menezes. On cryptographic protocols employing asymmetric pairings - the role of ψ revisited. *Discrete Applied Mathematics*, 159(13):1311–1322, 2011.
18. S. Chatterjee and A. Menezes. Type 2 structure-preserving signature schemes revisited. In *Advances in Cryptology ASIACRYPT 2015*, volume 9452 of *Lecture Notes in Computer Science*, pages 286–310. Springer Berlin Heidelberg, 2015.
19. J. Chen, H. W. Lim, S. Ling, H. Wang, and H. Wee. *Pairing-Based Cryptography – Pairing 2012: 5th International Conference, Cologne, Germany, May 16-18, 2012, Revised Selected Papers*, chapter Shorter IBE and Signatures via Asymmetric Pairings, pages 122–140. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
20. L. Chen, Z. Cheng, and N. P. Smart. Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 6(4):213–241, 2007.
21. P. Chen, X. Wang, and J. Su. A hierarchical identity-based signature from composite order bilinear groups. In *Algorithms and Architectures for Parallel Processing*, volume 9532 of *Lecture Notes in Computer Science*, pages 46–56. Springer International Publishing, 2015.
22. J. H. Cheon and T. Kim. A new approach to the discrete logarithm problem with auxiliary inputs. 19(1):1–15, 2016.
23. J. H. Cheon, T. Kim, and Y. S. Song. *Selected Areas in Cryptography – SAC 2013: 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, chapter A Group Action on $\mathbb{Z}_p^\times$ and the Generalized DLP with Auxiliary Inputs, pages 121–135. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
24. C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. *IEEE Trans. Parallel Distrib. Syst.*, 25(2):468–477, Feb. 2014.

25. H. Cohen and G. Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC Press, 2005.
26. J.-S. Coron and D. Naccache. *Advances in Cryptology - ASIACRYPT 2003: 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 – December 4, 2003. Proceedings*, chapter Boneh et al.'s k-Element Aggregate Extraction Assumption Is Equivalent to the Diffie-Hellman Assumption, pages 392–397. Springer Berlin Heidelberg, 2003.
27. A. Enge and J. Milan. Implementing cryptographic pairings at standard security levels. volume 8804 of *Lecture Notes in Computer Science*, pages 28–46. Springer International Publishing, 2014.
28. L. Fang, W. Susilo, C. Ge, and J. Wang. Public key encryption with keyword search secure against keyword guessing attacks without random oracle. *Information Sciences*, 238:221 – 241, 2013.
29. D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, 23(2):224–280, 2010.
30. E. S. V. Freire. Non-interactive key exchange and key assignment schemes. In *Phd Thesis inproceedingsinproceedingsStanford University*, 2014.
31. G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comput.*, 62(206):865–874, Apr. 1994.
32. S. D. Galbraith and P. Gaudry. Recent progress on the elliptic curve discrete logarithm problem. *Designs, Codes and Cryptography*, 78(1):51–72, 2015.
33. S. D. Galbraith, F. Hess, and F. Vercauteren. Aspects of pairing inversion. *IEEE Transactions on Information Theory*, 54(12):5719–5728, 2008.
34. S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Appl. Math.*, 156(16):3113–3121, 2008.
35. U. Ghosh and R. Datta. A secure addressing scheme for large-scale managed manets. *Network and Service Management, IEEE Transactions on*, 12(3):483–495, Sept 2015.
36. F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel. *On the Function Field Sieve and the Impact of Higher Splitting Probabilities*, pages 109–128. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
37. Y. Gong, Y. Cai, Y. Guo, and Y. Fang. A privacy-preserving scheme for incentive-based demand response in the smart grid. *Smart Grid, IEEE Transactions on*, (99):1–1, 2015.
38. R. Granger, T. Kleinjung, and J. Zumbrägel. *Breaking '128-bit Secure' Supersingular Binary Curves*, pages 126–145. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
39. R. Granger, T. Kleinjung, and J. Zumbrägel. On the discrete logarithm problem in finite fields of fixed characteristic. http://arxiv.org/abs/1507.01495, 2015.
40. F. Hess. Pairing lattices. In S. Galbraith and K. Paterson, editors, *Pairing-Based Cryptography Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 18–38. Springer Berlin Heidelberg, 2008.
41. L. Hitt. *Pairing-Based Cryptography – Pairing 2007: First International Conference, Tokyo, Japan, July 2-4, 2007. Proceedings*, chapter On the Minimal Embedding Field, pages 294–301. Springer Berlin Heidelberg, 2007.
42. D. Hofheinz and T. Jager. Tightly secure signatures and public-key encryption. *Designs, Codes and Cryptography*, pages 1–33, 2015.

43. J. Y. Hwang, D. H. Choi, H. Cho, and B. Song. New efficient batch verification for an identity-based signature scheme. *Security and Communication Networks*, 8(15):2524–2535, 2015.
44. A. Joux and K. Nguyen. Separating decision diffie–hellman from computational diffie–hellman in cryptographic groups. *Journal of Cryptology*, 16(4):239–247, 2003.
45. A. Joux and C. Pierrot. Technical history of discrete logarithms in small characteristic finite fields. *Designs, Codes and Cryptography*, 78(1):73–85, 2016.
46. T. Kim and R. Barbulescu. *Advances in Cryptology – CRYPTO 2016: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2012. Proceedings*, chapter Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
47. A. Kundu and E. Bertino. Privacy-preserving authentication of trees and graphs. *International Journal of Information Security*, 12(6):467–494, 2013.
48. N. P. S. L. Chen, Z. Cheng. Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 6(4):213–241, 2007.
49. K. Lee. Self-updatable encryption with short public parameters and its extensions. *Designs, Codes and Cryptography*, 79(1):121–161, 2016.
50. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. *Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 – June 3, 2010. Proceedings*, chapter Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, pages 62–91. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.
51. A. Lewko and B. Waters. *Advances in Cryptology – EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, chapter Decentralizing Attribute-Based Encryption, pages 568–588. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.
52. F. Li and P. Xiong. Practical secure communication for integrating wireless sensor networks into the internet of things. *Sensors Journal, IEEE*, 13(10):3677–3684, 2013.
53. F. Li, Z. Zheng, and C. Jin. Identity-based deniable authenticated encryption and its application to e-mail system. *Telecommunication Systems*, pages 1–15, 2015.
54. H. Li, Y. Dai, L. Tian, and H. Yang. *Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings*, chapter Identity-Based Authentication for Cloud Computing, pages 157–166. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
55. B. Libert, T. Peters, M. Joye, and M. Yung. Linearly homomorphic structure-preserving signatures and their applications. *Designs, Codes and Cryptography*, 77(2):441–477, 2015.
56. C. Liu, C. Yang, X. Zhang, and J. Chen. External integrity verification for outsourced big data in cloud and iot. *Future Gener. Comput. Syst.*, 49(C):58–67, Aug. 2015.
57. J. Liu, Z. Zhang, X. Chen, and K. S. Kwak. Certificateless remote anonymous authentication schemes for wirelessbody area networks. *Parallel and Distributed Systems, IEEE Transactions on*, 25(2):332–342, 2014.
58. Z. Liu, J. Li, X. Chen, J. Yang, and C. Jia. *Information Security and Privacy: 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, chapter TMDS: Thin-Model Data Sharing Scheme Supporting Keyword Search in Cloud Storage, pages 115–130. Springer International Publishing, Cham, 2014.

59. A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal. Secure and scalable cloud-based architecture for e-health wireless sensor networks. In *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*, pages 1–7, 2012.
60. H. Lu, J. Li, and M. Guizani. Secure and efficient data transmission for cluster-based wireless sensor networks. *Parallel and Distributed Systems, IEEE Transactions on*, 25(3):750–761, 2014.
61. F. Luca, D. J. Mireles, and I. E. Shparlinski. Mov attack in various subgroups on elliptic curves. *Illinois Journal of Mathematics*, 48(3):10411052, 2004.
62. M. Massierer. Some experiments investigating a possible L(1/4) algorithm for the discrete logarithm problem in algebraic curves. *IACR Cryptology ePrint Archive*, 2014:996, 2014.
63. A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *Information Theory, IEEE Transactions on*, 39(5):1639–1646, 1993.
64. D. Moody, R. Peralta, R. Perlner, A. Regenscheid, A. Roginsky, and L. Chen. Journal of Research of the National Institute of Standards and Technology. volume 120, pages 11–27. February 2015.
65. N. E. Mrabet, N. Guillermin, and S. Ionica. A study of pairing computation for elliptic curves with embedding degree 15. *IACR Cryptology ePrint Archive*, 2009:370, 2009.
66. L. Nkenyereye and K. Rhee. Secure traffic data transmission protocol for vehicular cloud. In *Advances in Computer Science and Ubiquitous Computing*, volume 373 of *Lecture Notes in Electrical Engineering*, pages 497–503. Springer Singapore, 2015.
67. A. M. Odlyzko. *Advances in Cryptology: Proceedings of EUROCRYPT 84 A Workshop on the Theory and Application of Cryptographic Techniques Paris, France, April 9– 11, 1984*, chapter Discrete logarithms in finite fields and their cryptographic significance, pages 224–314. Springer Berlin Heidelberg, Berlin, Heidelberg, 1985.
68. T. Okamoto and K. Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. *Designs, Codes and Cryptography*, 77(2):725–771, 2015.
69. S. C. Ramanna, S. Chatterjee, and P. Sarkar. *Public Key Cryptography – PKC 2012: 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*, chapter Variants of Waters' Dual System Primitives Using Asymmetric Pairings, pages 298–315. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
70. I. Semaev. New algorithm for the discrete logarithm problem on elliptic curves. *IACR Cryptology ePrint Archive*, 2015.
71. H. Shacham. *New Paradigms in Signature Schemes*. PhD thesis, Stanford, CA, USA, 2006.
72. H. Shacham and B. Waters. Compact proofs of retrievability. In *Advances in Cryptology - ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 90–107. Springer Berlin Heidelberg, 2008.
73. V. Shoup. *Advances in Cryptology — EUROCRYPT '97: International Conference on the Theory and Application of Cryptographic Techniques Konstanz, Germany, May 11–15, 1997 Proceedings*, chapter Lower Bounds for Discrete Logarithms and Related Problems, pages 256–266. Springer Berlin Heidelberg, Berlin, Heidelberg, 1997.

74. J. Tsai. A new efficient certificateless short signature scheme using bilinear pairings. *Systems Journal, IEEE*, PP(99):1–8, 2015.
75. Y.-M. Tseng, Y.-H. Huang, and H.-J. Chang. Cca-secure anonymous multi-receiver id-based encryption. In *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, pages 177–182, March 2012.
76. C. Wang, D. Shi, X. Xu, and J. Fang. An anonymous data access scheme for vanet using pseudonym-based cryptography. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–9, 2015.
77. H. Wang. Identity-based distributed provable data possession in multicloud storage. *Services Computing, IEEE Transactions on*, 8(2):328–340, 2015.
78. Y. Wang. *Transactions on Computational Science XVII*, chapter Efficient Identity-Based and Authenticated Key Agreement Protocol, pages 172–197. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
79. B. Waters. *Advances in Cryptology - CRYPTO 2009: 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, chapter Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions, pages 619–636. Springer Berlin Heidelberg, 2009.
80. Y. Xie and Y. Zhang. A secure, service priority-based incentive scheme for delay tolerant networks. *Security and Communication Networks*, 9(1):5–18, 2016.
81. P. Xu, Q. Wu, W. Wang, W. Susilo, J. Domingo-Ferrer, and H. Jin. Generating searchable public-key ciphertexts with hidden structures for fast keyword search. *Information Forensics and Security, IEEE Transactions on*, 10(9):1993–2006, 2015.
82. E. Zavattoni, L. Dominguez Perez, S. Mitsunari, A. Sanchez-Ramrez, T. Teruya, and F. Rodriguez-Henriquez. Software implementation of an attribute-based encryption scheme. *Computers, IEEE Transactions on*, 64(5):1429–1441, May 2015.

Appendix

A 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, 9, 18, 21, 27, 30, 35, 37, 43, 53, 57, 66, 74, 76, 81, 82]. These include the following applications:

Identity based encryption (IBE) [13]: 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) [11]: 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 [50, 51]: 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 [28]: 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 [10, 72]: 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 & 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 [72], internet of things (IoT) [52], e-health systems and wearable technologies [59].

Other applications: Last but not least, there are also various ID based mechanisms including authentication [16,54], identity based key-agreement [20, 78], 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).