CRITICAL PERSPECTIVES ON PROVABLE SECURITY: FIFTEEN YEARS OF "ANOTHER LOOK" PAPERS

NEAL KOBLITZ AND ALFRED MENEZES

Abstract. We give an overview of our critiques of "proofs" of security and a guide to our papers on the subject that have appeared over the past decade and a half. We also provide numerous additional examples and a few updates and errata.

Contents

Date: 10 June 2019; updated on 19 June 2019.

1. Introduction

What does "provable security" mean? If "proof" is understood in the strict mathematical sense — as in "proof of the Pythagorean Theorem" or "proof of Fermat's Last Theorem" — then there's a simple answer: There is no such thing. "Provable security" is an oxymoron. As Benjamin Franklin said 230 years ago, "in this world nothing can be said to be certain, except death and taxes." About communications security there can be no certainty.

But it is wrong to reject proofs in cryptography just because in general they do not measure up to the standards of pure mathematics. To take such an inflexible position would be, as Jonathan Katz pointed out, "snobbery at its purest" [201]. Proofs can be useful in several ways. They enforce a kind of discipline on authors so that they strive for precision, systematic approaches, and completeness. They rule out certain categories of attacks or attacks on certain parts of the protocol so that testing can focus on other types of attacks and on the assumptions made in the provable security theorem.

Proofs can also influence protocol design. If an obstacle is encountered in constructing a security reduction, that could indicate a potential point of attack, in which case a modification of the protocol might eliminate the vulnerability as well as remove the obstacle to the proof. On the other hand, modifications of protocols that are made for the purpose of getting proofs to go through can sometimes introduce new vulnerabilities to side-channel attacks and other threats that are outside the security model. This commonly happens when the modifications make the protocol more complicated.

Finally, as noted by Brian Snow [278, 217], security proofs help the adversaries, who then know better than to use their resources for the types of attacks that have been ruled out by the theorem.

In [210] we commented on the theorem/proof terminology:

> There are two unfortunate connotations of "proof" that come from mathematics and make the word inappropriate in discussions of the security of cryptographic systems. The first is the notion of 100% certainty. Most people not working in a given specialty regard a "theorem" that is "proved" as something that they should accept without question. The second connotation is of an intricate, highly technical sequence of steps. From a psychological and sociological point of view, a "proof of a theorem" is an

> intimidating notion: it is something that no one outside an elite of narrow specialists is likely to understand in detail or raise doubts about. That is, a "proof" is something that a non-specialist does not expect to really have to read and think about.
>
> The word "argument," which we prefer here, has very different connotations. An "argument" is something that should be broadly accessible. And even a reasonably convincing argument is not assumed to be 100% definitive. In contrast to a "proof of a theorem," an "argument supporting a claim" suggests something that any well-educated person can try to understand and perhaps question.

However, the terms "proof of security" and "provable security" are firmly established in the research community and are routinely used when discussing proposed protocols with the broader public. This can result in misunderstandings, since non-specialists might think that "proof" has the same meaning as in their high school and college math classes. A claimed proof can engender a false sense of security, and may discourage people from further study of the security of a protocol — why bother, since it has already been proven secure? Practitioners might not realize that a security proof was carried out under idealized assumptions and might incorrectly assume that the protocol necessarily retains its proven security when deployed in practice. In contrast to the mathematical meaning of "proof," in cryptography the word has a subtler and less straightforward meaning, a meaning that is conditional and contingent.

Provable security has four components: protocol description, definitions, assumptions, and the proof itself:

(1) We must give a precise description of all phases of the protocol, including parameter selection, key generation, and any subsidiary verification steps.
(2) We must define the adversary — what its goal is (for example, to determine, in time t with q queries and with a probability at least $\frac{1}{2} + \varepsilon$ of success, which of two messages has been encrypted), how it interacts with the protocol (perhaps through queries to honest users or by impersonating honest users), and what its computational capabilities are.
(3) We need to make explicit assumptions, for example, that factoring integers is hard, that a certain compression function is collision-resistant, or that a hash function behaves like an ideal random function.
(4) We finally give a formal proof, which shows that if the adversary succeeds in achieving its goal, then one of the stated assumptions must be false. We might give a security reduction that shows that the supposedly hard underlying mathematical problem can be solved efficiently by means of calls to the adversary (regarded as a subroutine or an oracle).

Ideally, there's also a fifth stage:

(5) We interpret the theorem as a certain type of useful guarantee, in which the assurance we give the practitioner is an accurate reflection of exactly what the theorem says.

Things can go badly wrong in many different ways:

(1) The protocol description might implicitly assume that something is of the proper form, whereas in reality that needs to be verified in order to avoid a certain type of attack (see §2).
(2) The definitions might not adequately model real-world adversaries. Cryptography is an unusual area of applied mathematics in that it deals not with natural phenomena but rather with malicious human opponents who are clever, devious, and powerful. There is a history of formal models of adversarial behavior falling far short of what real-world attackers are able to do (see §3).
(3) The evidence for the assumptions might be weak, and we might need to assume that certain components of the protocol behave in an ideal fashion (see §4).
(4) The proof might have a gap or fallacy, in which case the security assurance it provides completely disappears. Or the proof might be correct only in a non-standard model of computation that permits non-constructible algorithms, in which case the meaning of the proof in practice becomes highly problematic. Or the proof might be correct, but have a large "tightness gap," resulting in a guarantee that turns out to be meaningless for practical parameter sizes. (See §5.)

These are some of the questions we studied in our series of "another look" papers, starting in 2004, when "Another look at 'provable security'" [210] was posted. The purpose of this article is to give a road-map to those papers, focusing on some of the most important examples and controversies. At the same time we wish to update the papers with more recent examples and perspectives.

2. Deficient Protocol Descriptions

Sometimes a protocol description makes implicit assumptions concerning parameters, values that are sent, or formatting of messages. If these assumptions are not verified in the course of the protocol, an attacker might be able to achieve its goal by violating them. For example, in a key-exchange protocol, if Alice does not verify that the group element Bob sends her truly belongs to the large prime order subgroup rather than to a small subgroup or that the point that Bob sends her is really a point on the specified elliptic curve rather than on a curve having smooth group order, then Bob might be able to learn her secret key through a small-subgroup attack or an invalid-curve attack.

Moreover, gaps in a protocol description often carry over to the security proof itself. If a step in the protocol is "Bob sends Alice a group element," authors might construct security reductions implicitly assuming that Bob always sends Alice a group element. They might not notice that unless Alice performs a validation step that's not part of the protocol, she cannot know for sure that what Bob sent her is really an element of the group in question. This oversight could lead to a "provably secure" protocol that is actually insecure.

For example:

(1) In [103] Chen, Cheng, and Smart showed that the pairing-based key agreement scheme presented in [104] can be broken if subgroup membership testing is not performed.
(2) In [22] Bangerter, Camenisch, and Maurer presented a zero-knowledge protocol in which a user P proves knowledge of a (secret) discrete logarithm in a group of hidden order (such as the RSA group of order $\varphi(n)$) to a verifier V. The protocol and its security proof implicitly assume that the parameters selected by V in

the protocol satisfy certain conditions. However, Kunz-Jacques *et al.* [222] later showed that a dishonest V can learn P's secret if the parameters selected by V do not satisfy the conditions. This is a particularly serious flaw because no (efficient) method is known for verifying that the parameters satisfy the conditions.

(3) In [37] a method for batch verification of a modified version of the Digital Signature Algorithm (DSA) was proposed. (The purpose of batch verification is to enable a large number of messages signed with the same key to be verified together more rapidly than if verified individually.) The paper did not include a proof of security, but assured the reader that "...we can use the same techniques as before to prove that the tests are sound. Details omitted due to page limits." In the signature scheme the first component of the signature is an element of the order-q subgroup of the multiplicative group of integers mod p (where p and q are primes with $q \mid (p-1)$). The batch verification algorithm in [37] does not check that all the signatures in the batch have this property; and, in fact, it would be expensive to verify this. This omission was exploited by Boyd and Pavlovski [74] to break the batch verification of the modified-DSA signatures.

(4) In [82] it is noted that the direct anonymous attestation (DAA) scheme described in [109] and standardized by the International Organization for Standardization (ISO) fails to check that an issuer's credentials are not comprised of identity group elements. This omission allows any party to create valid DAA signatures on behalf of a trusted platform module (TPM), thus breaking the unforgeability requirement.

(5) In [167] Gong and Zhao showed that the one-pass authenticated key agreement protocol from ideal lattices presented in [300] could be easily broken if adversaries are able to get their maliciously-generated public keys certified by a certification authority. Indeed, Gong and Zhao argued that this is a plausible attack scenario since it seems difficult to distinguish maliciously-generated public keys from honestly-generated ones. The protocol description and proof of security in [300] had not taken account of the need for public key validation.

(6) When modifying a protocol, cryptographers should think twice before omitting a validation step. As part of his design of a variant of the MQV key agreement protocol [226] with a proof of security, Krawczyk [221] attempted to gain a performance advantage over MQV by omitting a public key validation step that seemed to be unnecessary for his proof. However, that step had been introduced in MQV in order to prevent a known attack. It turned out (see [237, 240]) that Krawczyk's security proof had some flaws, and certain versions of the HMQV protocol described in [221] were insecure because of the same attack that was prevented in MQV by the validation step.

3. Inadequate Definitions

In this section we list several examples of security definitions that are inadequate in some way. Sometimes the inadequacies are subtle and can take years to uncover. For example, in [39] (posted on eprint in 2009) Bellare, Hofheinz, and Kiltz noticed several discrepancies in the well-established security notion of indistinguishability under chosen-ciphertext attack (IND-CCA) for public-key encryption. They wrote:

> Our work shows that subtle foundational issues exist with notions that are supposedly well-established and unambiguous, and highlights the need to be careful and precise with regard to "minor" definitional "details."

3.1. **Side channels.** A side-channel attack uses physical observation of hardware or analysis of error messages to infer information about secret bits. The attack might exploit variations in time, power consumption, or electromagnetic radiation as the device carries out an algorithm; it might measure responses to formatting errors or induced faults; it might exploit information leaked about access patterns of a CPU's memory cache; it might use bugs or peculiarities in the programming; or it might use a combination of different types of leaked information. For example, in 2001 Manger [234] developed a successful chosen-ciphertext attack on a certain version of RSA encryption (RSA-OAEP). The Manger padding attack uses information learned when ciphertexts are rejected, such as the time it took the decryption to fail or the nature of the error messages that were returned.

The conventional definition of security for a MAC scheme is existential unforgeability under chosen-message attacks (where the adversary is given access to a MAC oracle). In practice, an adversary might also have access to a tag-checking oracle (which decides whether a given message-tag pair is valid). Bellare-Goldreich-Mityagin [38] proved that the tag-checking oracle does not change the adversary's ability to produce a forgery.

Interestingly, there is a very practical timing attack on MAC schemes [293] that measures the time it takes to verify the tag of a message. The danger from such a timing attack would not be considered by the designer of a MAC scheme if the designer was using a security model that does not allow verification queries.

A particularly bothersome feature of side-channel attacks is that a countermeasure taken to reduce risk from one type of side-channel leakage might increase vulnerability to other types of attacks. A common recommendation to avoid timing and power-consumption attacks is to introduce dummy steps so that operations with a 0-bit of the secret key are indistinguishable from operations with a 1-bit. However, the use of dummy steps may enable an induced-fault adversary to detect the location of the 0-bits because an induced fault during a dummy step will not affect the output, while a fault induced during a necessary operation will. For details see the survey [138].

Although side-channel attacks have played an important role in cryptography at least since the 1940s, there were no serious attempts to model such attacks until the 2000s. The most prominent such model, called *leakage resilience*, aims to capture *all* possible side-channel attacks. In [217] we examined this model and found it to be woefully inadequate.

Leakage resilience theorems typically assume a certain upper bound on the number of leaked bits, e.g., 50% of the bits of a private key. In the real world, how could one possibly get an assurance that all attacks will satisfy this bound? The effectiveness of side-channel attacks depends on many factors that are external to the protocol — the physical construction of the device, proximity of the adversary, and details of system-level implementation. A leakage resilience theorem is only likely to give practitioners a false sense of security. In [217] we suggested that it is hopeless to try to give a formal model that encompasses side-channel attacks, and that one has no choice but to use *ad hoc* countermeasures.

A protocol that's modified so as to provide leakage resilience — for example, so as not to lose security if 50% of a private key is leaked — is likely to be much less efficient and much more complicated than the original protocol. The leakage-resilient protocol has more attack points, and it becomes more difficult to add practical countermeasures as the protocol becomes more complex.

3.2. **Padding — SSL/TLS.** Before encrypting a plaintext (in either symmetric or asymmetric encryption) one normally appends a prescribed amount of random padding and formatting. Randomness counteracts dictionary and chosen-plaintext attacks. Formatting can reduce the effectiveness of chosen-ciphertext attacks, since the decryption of the adversary's ciphertext is likely to violate the formatting, in which case the adversary will receive an error message rather than plaintext. However, on several occasions the padding and formatting have been exploited by side-channel attacks that analyze timings or error messages and thereby recover parts of the plaintext. In §3.5-3.6 of our paper "Another look at security definitions" [217], we discussed some attacks on widely used symmetric encryption protocols, focusing mainly on SSH.

In this section we summarize some curious episodes in the history of SSL/TLS protocols with Cipher Block Chaining (CBC), which have been the standards for encryption over the internet. (For an explanation of CBC, see §3.5 of [217].) What we'll see is a history of security results being proved for models of SSL/TLS that left out implementation details that were later exploited in real attacks. Subsequently both the protocol and the model in the proof were changed to rule out those attacks; and then the cycle repeated.

In 2001, Krawczyk [220] proved that if CBC is used for encryption, then the process used in TLS 1.0 (1999) of applying a message authentication code (MAC) followed by encryption is secure as an authenticated encryption scheme. In the abstract of [220] he assured users that "...the current practical implementations of the [SSL/TLS] protocol that use the above modes of encryption are safe." Herley and van Oorschot [177] warn against giving this kind of guarantee to the public: "Speaking of mathematical guarantees as if they are properties of real-world systems is a common error." In fact, Krawczyk's proof had made some simplifications — omitting the padding and using a new random initialization vector (IV) for each packet.

In 2003, Canvel, Hiltgen, Vaudenay, and Vuagnoux [90] (see also Vaudenay [289]) presented a chosen-ciphertext attack on the TLS authenticated encryption scheme, in which an adversary can determine some of the plaintext corresponding to a target ciphertext. The attacker queries altered versions of the target ciphertext and learns (perhaps through time measurements) whether the recipient rejects the query because of incorrect padding or because of an incorrect MAC tag (as happens when the padding is correct). This attack, called a "padding oracle attack," is similar to Manger's attack on RSA-OAEP (see §3.1). As explained by Degabriele, Paterson, and Watson [129], "Krawczyk's proof is mathematically correct, but his model doesn't accurately capture the way SSL/TLS works in practice.... This means that...it can't be applied directly to the protocol as specified."

In 2006, version 1.1 of TLS attempted to address this padding oracle attack by changing the decryption algorithm so that, if the padding is incorrect, it proceeds to decrypt as if there's not supposed to be any padding; then the rejection occurs later, when the MAC tag fails to verify. Although this removed most of the processing time difference between correct and incorrect padding, it didn't remove it entirely, because with the padding

absent there were more message blocks to decipher. However, it was felt that this timing difference would be too small to exploit in a practical timing attack.

In 2011, Paterson, Ristenpart and Shrimpton [252] introduced the notion of "length-hiding authenticated encryption security" and proved (under certain assumptions) that the TLS 1.1 authenticated encryption scheme satisfied this notion. They warned that their security definition is in the "uniform-error reporting model" (where decryption does not reveal the cause of any failure) and so their security proofs "don't necessarily apply when non-uniform reporting is in effect."

In 2013, AlFardan and Paterson [10] presented an intricate timing attack on the authenticated encryption scheme in TLS 1.1. They wrote that "our attacks do not contradict the results of [252], but instead relativize their applicability to practice." In other words, the attacks show that the results of [252] don't apply to practice.

In 2011, Duong and Rizzo [135] presented their BEAST attack (Browser Exploit Against SSL/TLS) on TLS 1.0 that exploits the fact that the last ciphertext block is used as the IV for the next encryption. In 2014, Möller, Duong and Kotowicz [242] presented their POODLE attack (Padding Oracle On Downgrade Legacy Encryption) on the authenticated encryption scheme in SSL 3.0 (where, unlike in TLS 1.0, the content of the padding bytes was not specified). Their attack exploits the fact that the last padding byte is the length of the padding. Finally, after all the trouble with CBC-mode encryption, the most recent version TLS 1.3 (2018) mandates the use of Galois Counter Mode (GCM) instead.

3.3. **Symmetric-key encryption.** A symmetric-key encryption scheme is required to be secure against chosen-plaintext attacks, in which an adversary is allowed to query an encryption oracle with plaintext messages of the adversary's choosing. The standard definitions of security all stipulate that the adversary presents a whole plaintext to the encryption oracle, which responds with the corresponding ciphertext. However, Joux, Martinet, and Valette [198] noticed a striking deficiency in these security definitions. Namely, they observed that in some applications, such as encryption with a smart card, the adversary might be able to send blocks of a plaintext one at a time to the smart card and immediately receive the ciphertext block. In this way, the adversary can select the next plaintext block based on the ciphertext blocks previously received. Joux *et al.* demonstrated that CBC encryption is insecure against such "blockwise-adaptive" chosen-plaintext attacks. They also showed that a provably secure authenticated encryption scheme in [172] is insecure against blockwise-adaptive chosen-plaintext attacks, and a provably secure hybrid encryption scheme in [119] is insecure against blockwise-adaptive chosen-ciphertext attacks.

3.4. **Encrypted databases.** Encrypted databases employ specialized encryption schemes to allow a database server to perform useful operations on encrypted data. Grubbs *et al.* [170] showed that the security definition in [259] for multi-key searchable encryption is inadequate for passive as well as active attacks, and presented an attack on the Mylar encrypted database that employs multi-key searchable encryption. Grubbs, Ristenpart, and Shmatikov [171] argue that the notion of a "snapshot attacker," who can only obtain a snapshot of a database at a given point in time, is inadequate for modeling security for encrypted databases, and hence provable security claims like the one in [257] are meaningless. The paper [171] highlights the difficulty of employing provably-secure property-revealing encryption schemes such as deterministic encryption [30] and order-preserving encryption [65] in fully functional encrypted database management systems. The authors of [171]

conclude that members of systems conference program committees who review papers on encrypted databases should be "very skeptical of claims of 'provable confidentiality,' especially if not supported by a thorough security evaluation...."

3.5. **Signatures.** Sometimes an accepted model for security of a type of protocol turns out many years later to be inadequate for applications that were never anticipated in the era when the security definition was devised. What is still considered the standard security definition for a signature scheme — unforgeability under adaptive chosen-message attack — was proposed in 1984 by Goldwasser, Micali, and Rivest (GMR) [165]. As explained in [217], in the pre-internet days no one foresaw such applications as online auctions, lotteries, and cryptocurrencies. People thought of digital signatures simply as improved versions of written signatures that would be used for the same purposes. In particular, there was no need to worry about adversaries claiming someone else's signature as their own — with traditional signatures, no one would have a motive to do that.

However, consider an online lottery where users digitally sign their chosen lottery number; then Alice claims her winnings by producing her certified public key that is then used to verify that the winning number is hers. Suppose that, between the time when the winning number is announced and Alice shows up to claim the money, Bob is able to select and certify a key pair such that the same lottery number has the same signature under his key as under Alice's. If he can do that, he can claim Alice's winnings before Alice does. This is called a Duplicate Signature Key Selection (DSKS) attack [60, 239, 217]. It turns out that some (but not all) signature schemes secure in the Goldwasser-Micali-Rivest sense can fall victim to the DSKS attack. Interestingly, RSA with variable encryption exponent e is vulnerable, whereas RSA with fixed e is not. Although conventional wisdom says that randomness in parameter selection increases security — in which case RSA with e randomly generated for each user would be more secure than system-wide $e = 3$ or $e = 65537$ — the opposite is true if one needs protection from DSKS. Allowing more variability in key selection plays to the advantage of the DSKS adversary.

3.6. **Key agreement.** The widely accepted definition of security of a key agreement protocol is due to Canetti and Krawczyk [86, 87, 88]. It is powerful because it allows for various forms of corruption and ill-intentioned queries by the adversary. However, as explained in [237], it does not consider key-compromise impersonation (KCI) attacks. Suppose that an adversary Chris wants to obtain secret information from Alice that Alice is only willing to share with a second user Bob. Chris succeeds in capturing Alice's secret key (but not Bob's). His task then is to make use of Alice's secret key to impersonate Bob to Alice. Some (but not all) key agreement protocols that are secure in the Canetti-Krawczyk sense are not secure against a KCI adversary.

3.7. **Single-user assumption.** In practice, cryptography is almost always deployed in an environment with many users. An adversary may choose to broadcast a simultaneous attack against a large number n of them. Even if its probability of success with a given user is only ε, it often happens that with roughly the same expenditure of resources the adversary's chance of compromising at least one of its targets is $n\varepsilon$. From the perspective of a single user Alice, ε might be an acceptable level of risk, but from the standpoint of the system as a whole the $n\varepsilon$ probability of a successful attack might not be.

Curiously, the classic definitions of security for symmetric-key encryption, symmetric-key message authentication, public-key encryption, and signatures were all in the single-user setting. A security reduction in that setting can usually be carried over to the multi-user setting. However, in many cases this results in a large "tightness gap" that can cause the practical assurance provided by the reduction to have little value. We will give several examples of this in §5.4.2.

3.8. **Password authentication.** In [174] Halevi and Krawczyk proposed a challenge-response password authentication protocol, in which a user demonstrates knowledge of a secret password to a server. They prove that the protocol is secure (and, in fact, that it has optimal resistance to off-line password guessing attacks) under the assumption that the underlying public-key encryption scheme satisfies a weak notion of chosen-ciphertext security, namely resistance to "one-ciphertext verification" attacks. The security proof is in the single-user setting.

Soon after, Boyarsky [72] showed that the Halevi-Krawczyk protocol is sometimes insecure if the adversary poses as a second user. Boyarsky designed a public-key encryption scheme — a slightly simplified version of a public key encryption scheme of Dolev-Dwork-Naor [132] — that resists one-ciphertext verification attacks. In [72] it was shown that an adversary who observes an execution of the password authentication protocol between an honest user Alice and the server can then learn Alice's password by posing as a second user Bob and interacting with the server. Such attacks were not considered in the Halevi-Krawczyk security model for password authentication, in which the adversary is allowed to interact with the server only if it poses as Alice.

3.9. **Safety margins.** Sometimes certain features of a protocol are not known to be absolutely necessary, but rather function as a safety margin. In §5 of [217] we commented:

> One reason for including "extra" validation steps in a protocol is that they might help in the event of attacks that are not anticipated by the security model. For example, suppose that the digital signature standards had mandated that the sender include his public key in the message and the recipient verify that it's there. It was shown in [239] that this would have thwarted the standard Duplicate Signature Key Selection attacks. Or, alternatively, suppose that all signatures had to be timestamped, all certificates issued by a CA also had to be timestamped, and verification of a signature included checking that the certificate's timestamp precedes the one on the signature. Such a requirement — which might be an unreasonable imposition in some settings because a reliable clock is not always available — also would have prevented DSKS attacks. But neither inclusion of the public key in the message nor timestamping is required by the GMR security model; nor is either required by any of the commonly-used digital signature standards.

Moreover, as we saw in §2, omitting a public key validation step can easily result in a fallacious proof and an insecure protocol.

Other examples of safety margins include requiring that an encryption scheme satisfy the standard notion of chosen-ciphertext security rather than one-ciphertext security in

the Halevi-Krawczyk password authentication scheme (see §3.8), and including public keys in the hash in Schnorr signatures (see §5.4.2).

3.10. **More problems with deficient definitions.** Security proofs for many types of protocols have run into problems because of inadequate definitions. Below we list various types of protocols followed first by a reference to a paper or papers claiming provable security results and next by a reference to the paper or papers that found fault with these claims because of problems with the security model.

(1) Lightweight identification protocol [199] [161].
(2) Direct anonymous attestation (DAA) [77, 78, 101] [50, 83].
(3) Group key establishment [76, 75] [63].
(4) Universally composable signatures [89] [17].
(5) Blind signatures [258] [269].
(6) Designated confirmer signatures [84, 166, 159] [291].
(7) Public-key encryption with keyword search (PEKS) [69] [1].
(8) Multi-recipient encryption [31] [256].
(9) Revocable identity-based encryption [67] [271].
(10) Robust encryption [2] [139].
(11) Symmetric-key encryption schemes that are resistant to mass surveillance [43] [128].

4. Bodacious Assumptions

In [213, 214] we described an increasing tendency to base protocols on problems for which there is little evidence of hardness. In many cases these assumptions are contrived and unnatural, are not of interest except in studying a certain specific protocol, and have never before been studied. In some cases the intractability assumption is nothing but a thinly disguised version of the adversary's task, so that the security reduction becomes little more than a trivial tautology. According to Goldwasser and Kalai [164],

> We believe that the lack of standards in what is accepted as a reasonable cryptographic assumption is harmful to our field. Whereas in the past, a break to a provably secure scheme would lead to a mathematical breakthrough, there is a danger that in the future the proclaimed guarantee of provable security will lose its meaning. We may reach an absurdum, where the underlying assumption is that the scheme itself is secure, which will eventually endanger the mere existence of our field.

In [212] we pointed out that there is not much incentive to devote effort to studying an unnatural problem if its assumed hardness only implies — and is not equivalent to — security of the protocol:

> From the standpoint of someone who's thinking about studying a nonstandard problem such as the various interactive versions of the DLP [Discrete Log Problem], there is a disincentive to do so if the reduction goes only one way, that is, if the "hard" problem might be strictly easier than a successful attack on the protocol.... [S]uppose that a cryptanalyst works hard to develop a faster-than-expected algorithm for a non-standard DLP-type problem used in a security proof, and that this does not break the protocol,

> but only calls into question the assurance given by one particular proof. The danger (from the point of view of the analyst) is that the promoters of the protocol will point out that their protocol has not been broken, and then quickly give a new "proof of security" based on a slightly different problem — in which case the researcher's algorithm no longer has any relevance. If the non-standard problem was of little interest except for its appearance in the earlier "proof of security" (now superceded), then the cryptanalyst might justifiably feel resentment about having wasted time developing an attack on the problem. So if one wants to encourage intensive research on an underlying "hard" problem, it's best if the problem is *equivalent* to a successful attack.

4.1. **A history of broken assumptions.** Despite the lack of incentive to try to find fast algorithms for unnatural problems, there have been several cases where researchers did study those problems and found them to be significantly easier to solve than had been thought.

(1) In [169] Groth showed how a tighter security reduction for certain signature schemes could be obtained by assuming hardness of the problem of finding roots of elements in subgroups of $\mathbb{Z}_n^*$ of hidden order. For a subgroup of order 2^{2t}, his assessment was that the fastest attack takes time 2^t. However, Coron *et al.* [121] found attacks that take time $2^{t/2}$.
(2) In [184] the authors gave a security reduction for their public-key encryption scheme based on the problem of finding roots of a family of multivariate quadratic equations over a finite field, where the coefficients of the equations are selected according to a certain distribution. In [7] Albrecht *et al.* found practical attacks on the new problem. For two parameter sets that were proposed in [184] and were claimed to provide at least 80 bits of security, the attacks in [7] recovered the private key in 5 minutes and 30 minutes.
(3) In [112] the authors introduced the co-approximate common divisor problem (co-ACD) in connection with their proposal for an efficient additive homomorphic public-key encryption scheme. In [142] Fouque *et al.* described lattice attacks on co-ACD that resulted in key recovery in a few seconds for parameters that were intended to provide 128 bits of security.
(4) In [66] the authors supported the security of their pairing-based sequential aggregate signature scheme by giving an exponential lower bound in the generic group model for a certain "Modified Lysyanskaya-Rivest-Sahai-Wolf" (M-LRSW) problem. In [189] Hwang *et al.* showed that the proof of the lower bound was wrong and both the problem and the signature scheme can be easily broken. (More details are given in our papers [213, 214].)
(5) In [179] a ring variant of the learning parity with noise problem (Ring-LPN) was proposed, and was used as the basis for an authentication protocol suitable for resource-constrained devices such as RFID tags. Shortly after, Bernstein and Lange [56] devised an attack on Ring-LPN that violated the security claims in [179]. It is not clear whether Ring-LPN based protocols have any advantages at all over conventional AES-based ones.

(6) In 2013, Garg, Gentry, and Halevi [154] gave the first construction of an (approximate) multilinear map. This led to a flurry of activity. Multilinear maps were used to design protocols for many cryptographic tasks, including one-round multi-party Diffie-Hellman key exchange and indistinguishability obfuscation. However, the underlying security assumptions on the multilinear maps were new and not well studied. Indeed, the four variants of the so-called Graded Decisional Diffie-Hellman (GDDH) assumption for multilinear maps that were proposed as a basis for security claims in [154, 123, 158, 124] were found to be false in [183, 111, 122, 110], respectively. The attacks on the GDDH problem also led to attacks on several schemes for indistinguishability obfuscation; see [288] for a summary.

(7) The papers [41, 42, 64] used the "one more discrete log problem" (1MDL) and "one more Diffie-Hellman problem" (1MDH) to prove the security of blind signature schemes and Schnorr's identification scheme. Here the 1MDL problem is the problem of finding $\ell + 1$ discrete logs using a discrete-log oracle that answers ℓ queries, and similarly for the 1MDH problem. In [214] we commented:

> At first it might seem that these problems should be equivalent in difficulty to the problem of finding the discrete log of a single random element or finding the Diffie-Hellman element Z for fixed X and a single random Y. However, it turns out that this depends very much on what groups are used. In [212] we studied these problems and several others in the setting of the jacobian group of a genus-g curve. Assuming that one uses current state-of-the-art algorithms, we found that 1MDL is harder than 1MDH for $g = 1, 2$, whereas Granger [168] recently observed that the two problems are of roughly equal difficulty for $g \geq 3$; and it is only for non-hyperelliptic curves of genus 3 that the two problems are no easier than the DL and DH problems. Note that reductions are not known from 1MDH to 1MDL or from 1MDL to 1MDH. Our conclusion was that it is often unclear how to gauge the true level of difficulty of an interactive problem or one with complicated input.

(More details are given in §7 of [214].)

4.2. **Idealized models.** It sometimes happens that, in order to get a security reduction for a protocol, researchers have to adopt an idealized model for one of its basic components. That is, one assumes that a certain ingredient in the protocol functions in such a way as to reveal absolutely no information other than what's necessary in order to do its job — everything else looks purely random to an adversary. Since no actual implementation functions this way, Bernstein [51] has suggested that it's best to think of this not as "modeling" a component of the protocol, but rather as stipulating that an attack will not exploit any features of that part of the protocol.

The use of an idealized model by itself does not necessarily lead to a security result that has poor applicability to real-world cryptography. On the contrary, in the case of one of the most important idealized models — random oracles — we have argued that their use in security proofs is relatively innocuous. Moreover, it is generally not a good idea to replace a simple protocol by a more complicated one for the sole purpose of avoiding random oracles in a security reduction argument.

4.2.1. *Random oracles.* The random oracle model (ROM) is a powerful tool introduced by Bellare and Rogaway in [45] in order to make it possible to prove security for certain basic cryptographic protocols, such as Full Domain Hash signatures [45] and OAEP encryption [46].

Typically it is a hash function that is modeled by a random oracle. Informally speaking, this means that one regards the hash function h as a black box that responds to a query for the hash value of a bitstring m by giving a random value. For each query the oracle makes an independent random choice, except that it keeps a record of its responses and repeats the same response if m is queried again. The random oracle assumption is much stronger than collision-resistance, preimage resistance, the pseudorandom function property, and other properties that are commonly assumed to hold for hash functions in various applications. Some, such as Canetti, Goldreich, and Halevi [85], have argued that it is too strong, and have supported this viewpoint by devising protocols that are provably secure in the random oracle model but insecure in any concrete instantiation.

Starting in [210], we have argued that there is no convincing evidence of failure of the random oracle model. Despite researchers' best efforts, the only examples of failure have been contrived protocols that have no relation to practice because they violate obvious cryptographic principles. In a more recent article [219] we returned to this topic and concluded that in more than two decades of study no strong reason has emerged to believe that security reductions using random oracles are more unreliable than security reductions that use "standard" assumptions. We also believe that the use of the word "standard" for assumptions that avoid random oracles is misleading, since many of those assumptions are complicated, unnatural, little studied, and specially designed for a small set of protocols. We prefer the neutral terms "ROM protocol" and "non-ROM protocol," respectively, for protocols whose only known security reductions require the random oracle model and for protocols whose security can be proved without using that model.

Many papers have been devoted to constructing new or modified protocols that have security reductions without random oracles; as of the end of 2018 Google Scholar listed 300 articles having "without random oracles" in the title. However, in some cases the non-ROM protocols constructed to avoid what is basically a theoretical issue are more complicated than the earlier ROM protocols and are more vulnerable to attacks that are outside the security model.

For example, in [217] we noted that while RSA signatures with fixed encryption exponent e are not susceptible to the Duplicate Signature Key Selection attack (DSKS, see §3.5 above), the variant developed by Gennaro-Halevi-Rabin [157] in order to avoid random oracles is totally susceptible. The GHR scheme works as follows. Suppose that Bob wants to sign a message m. His public key consists of an RSA modulus n and a random integer t; here $n = pq$ is chosen so that $(p-1)/2$ and $(q-1)/2$ are prime. Let $h(m)$ be the hash value, which we assume to be odd. Bob now computes $\tilde{h}$ such that $\tilde{h}h \equiv 1 \pmod{p-1}$ and $\pmod{q-1}$. His signature s is $t^{\tilde{h}} \pmod{n}$. Alice verifies Bob's signature by computing h and then $s^h \bmod n$, which should equal t.

But an adversary who wants to steal Bob's lottery winnings by claiming s as his own signature on m need only find (n', t') such that $s^h \equiv t'$ modulo n'. This is trivial, since n' can be chosen arbitrarily and then t' can be set equal to s^h modulo n'.

Another example of trouble with non-ROM protocols relates to side-channel attacks (see §3.1 above) on pairing-based protocols. It is a remarkable fact (see [98] and §5 of [217]) that essentially the only such protocols that are known to be directly vulnerable to induced-fault attacks on pairing computations are those that were constructed specifically as non-ROM alternatives to earlier ROM-protocols. This is no accident, since the very same feature of the protocol makes possible both the non-ROM proof and the susceptibility to induced fault attacks. After a great deal of effort was devoted to developing a way around what seems to have been only a theoretical problem, we find that the modified protocols have increased vulnerability to certain types of realistic side-channel attacks.

4.2.2. *Generic groups.* Let G be a cyclic group of prime order q, and let g be a generator. The map $i \mapsto g^i$ gives a one-to-one correspondence between integers mod q and group elements; the discrete log problem is the problem of inverting this map. Shoup [273] introduced a "generic" model for such a group, so that he could prove that discrete logs could not be found in fewer than $O(\sqrt{q})$ steps using generic algorithms.

In the generic group model we have no information related to where the group "comes from" (e.g., points on a particular elliptic curve). Rather, we have an oracle that for any i gives us an "encoding" $\sigma(i)$ of the corresponding group element. In addition, if we have two encodings $\sigma(i)$ and $\sigma(j)$ (but we do not necessarily know i or j) and integers $0 \leq r, s < q$, we can ask the oracle for the encoding $\sigma(ri + sj)$. The oracle's encodings are randomly selected elements from some set of bitstrings. The only condition on the oracle's responses is that if the same group element is queried a second time, it must respond with the same encoding.

In [211] we commented that the generic group model is farther removed from reality than the random oracle model. A well-designed hash function has no perceptible structural feature that could ever be exploited by an adversary. In contrast, the groups used in cryptography all have structural elements that could possibly be of use in some kind of attack. For example, the group in DSA is a subgroup of the nonzero residues mod p. Elliptic curve groups over a binary field have subsets of points whose x-coordinate is represented by a low-degree polynomial. The generic group assumption in such cases is very strong, since it says that no adversary will ever find a way to use these features. (It should be noted that confidence in the security of cryptosystems based on a suitably chosen elliptic curve defined over a prime field rests not on the generic group assumption, but rather on three decades of work analyzing possible concrete attacks.)

For this reason a protocol should not be advertised as secure under "standard" assumptions — that is, secure without random oracles — if confidence in its security requires the generic group assumption. In [211] we questioned whether the Boneh-Boyen construction in [68] of a non-ROM scheme with short signatures was really a step forward. The whole point of the construction was that the scheme has a security proof without random oracles. However, the mathematical problem m-SDH (Strong Diffie-Hellman) whose hardness is assumed in the proof is a somewhat exotic and unnatural variant of the Diffie-Hellman assumption; and the evidence of its hardness given in [68] requires the generic group assumption, which is arguably a much stronger assumption than the random oracle assumption that the protocol was designed to avoid.

Similarly, the papers [148, 147] present efficient blind signature schemes which, the papers' titles promise, are proven secure in the "standard model." However, both blind signature schemes employ the "structure-preserving signature scheme on equivalence classes" from [149]. The only known security proof for the latter scheme is in the generic group model. Thus, the use of the word "standard" to describe the security assumptions in [148, 147] is misleading.

4.2.3. *Ideal ciphers.* The ideal cipher model does for symmetric encryption what the random oracle model does for hash functions. That is, it makes it possible to prove security of hybrid schemes under the assumption that the symmetric encryption component cannot be exploited by the adversary.

This model consists of an encryption oracle and a decryption oracle. Both oracles keep records of their own queries and responses, as well as those of the companion oracle. The input to the encryption oracle is a key k and a message block m, and the output is a random ciphertext block c that is the same as an earlier response to a query with the same key if and only if the message part of that query was also the same; and c is equal to the ciphertext part of an earlier decryption query with the same key if and only if the response to that query was the m in the encryption query. The decryption oracle takes input of the form (k, c) and outputs a random plaintext block m that is the same as an earlier response to a query with the same key if and only if the ciphertext part of that query was also the same; and m is equal to the message part of an earlier encryption query with the same key if and only if the response to that query was the c in the decryption query. In other words, the only requirement is that encryption and decryption must be inverse processes.

In 2005, Coron *et al.* [118] showed that an ideal cipher can be used to construct a hash function that is "indifferentiable" from a random oracle. Roughly speaking, this means that any cryptographic protocol that is secure in the random oracle model remains secure when the random oracle model is replaced by the hash function that is constructed from an ideal cipher.

In 2008, Coron, Patarin, and Seurin [126] showed that a random oracle can be used to construct a block cipher that is indifferentiable from an ideal cipher. The cipher is constructed by means of 6 Feistel rounds (also known as Luby-Rackoff rounds). In [126] they say:

> Our result shows that the random oracle model and the ideal cipher model are actually equivalent assumptions. It seems that up to now, many cryptographers have been reluctant to use the Ideal Cipher Model and have endeavoured to work in the Random Oracle Model, arguing that the ICM is richer and carries much more structure that the ROM. Our result shows that it is in fact not the case and that designers may use the ICM when they need it without making a stronger assumption than when working in the random oracle model. However, our security reduction is quite loose, which implies that in practice large security parameters should be used in order to replace an ideal cipher by a 6-round Luby-Rackoff. (p. 3)

In [182] (see also [120]), the authors show that the proof in [126] is incorrect. Instead they give a 14-round Feistel construction of a block cipher from a random oracle that

is indifferentiable from an ideal cipher. However, their security reduction has a large tightness gap (see §5.4).

5. Problematic Proofs

5.1. **Fallacious proofs.** The central role of "proofs" of security is a relatively recent phenomenon in the history of cryptographic practice, dating roughly to the late 1990s (although security reductions can be found in the literature much earlier). According to Katz and Lindell [202] and Goldreich [162], it is rigorous proof methodology that has been transforming cryptography "from an art to a science." A rigorous proof, they maintain, is the only way to get an ironclad guarantee; anything short of a proof is merely "heuristic" or "*ad hoc*." Because this viewpoint has been dominant at the most prestigious crypto conferences for many years, anyone who proposes a new protocol should expect sharp criticism and rejection if it is not accompanied by a proof of security.

For those who view a reductionist security proof as the gold standard for confidence in a protocol it logically must follow that a fallacious proof is a serious matter. In mathematics, a fallacy in a proof means that you have no proof at all. The ironclad guarantee simply evaporates. One of the central appeals we make in our "another look" papers is to please not try to have it both ways. You can't say that formal proofs are very important, and then say that fallacies in proofs are not important. Bernstein [53] has lamented "the security impact of a continuing series of errors" in security proofs, and has commented in reference to a flawed proof that "this avalanche of errors raises a much larger question: what protection does the cryptographic standardization process have against errors in provable-security claims?"

When confronted with an error in a security reduction we must try to determine what it signifies. There are several possibilities:

(1) The error can be patched and the original proof restored; or a different proof with no flaw can be given of exactly the same result. Perhaps a (hopefully minor) modification can be made in the protocol that enables the proof to be fixed.
(2) Another proof can be given of a weaker result, perhaps with stronger assumptions or a larger "tightness gap" (see §5.4). If we're lucky, the weakening of the result will be mainly of theoretical interest and will not cause security concerns for practical implementations.
(3) No satisfactory reductionist proof can be found, but there's a really convincing heuristic argument that in practice seems to rule out the same attacks as the earlier claimed result.
(4) The flaw in the proof is an essential one from a practical standpoint, because there is a realistic attack that shows that the claimed theorem is false.

Until we determine otherwise, we should assume the worst — the last possibility in this list — and should not try to minimize the importance of the flaw.

It is largely the disciplinary culture of our community (see [205, 206]) that explains the embarrassing fact that proofs — even proofs by eminent researchers for protocols that have practical importance — are often fallacious. Researchers, especially in academia, feel tremendous pressure to generate large numbers of publications so as to consolidate their own reputation and help their collaborating graduate students and post-docs get good jobs. These publications usually appear in conference proceedings, which have strict

TABLE 1. Major provable security claims found to have fallacies in the proofs.

Type of protocol	Paper with purported proof	Paper explaining fallacy
1) Public key encryption padding (OAEP)	Bellare-Rogaway Eurocrypt 1994 [46]	Shoup 2002 [275]
2) Signature schemes	Coron Eurocrypt 2002 [117]	Kakvi-Kiltz 2012 [200]
3) Identity-based encryption	Boneh-Franklin SIAM J. Comp. 2003 [70]	Galindo 2005 [152]
4) Authenticated encryption (GCM)	McGrew-Viega Indocrypt 2004 [236]	Iwata-Ohashi-Minematsu 2012 [194]
5) Key agreement (HMQV)	Krawczyk Crypto 2005 [221]	Menezes 2007 [237]
6) Message authentication codes (CBC-MAC and EMAC)	Bellare-Pietrzak-Rogaway Crypto 2005 [44] and Pietrzak ICALP 2006 [255]	Jha-Nandi 2016 [196]
7) Triple encryption	Bellare-Rogaway Eurocrypt 2006 [47]	Gaži-Maurer 2009 [156]
8) Symmetric encryption (XLS)	Ristenpart-Rogaway FSE 2007 [261]	Nandi 2014 [246]
9) Tweakable encryption	McGrew-Fluhrer SAC 2007 [235]	Chakraborty–Hernández-Jiménez–Sarkar 2015 [91]
10) Random oracles and Ideal ciphers	Coron-Patarin-Seurin Crypto 2008 [126]	Holenstein-Künzler-Tessaro 2011 [182]

submission and reviewing deadlines, so authors are rushed when writing their papers, and reviewers are rushed when evaluating them. As a result, reviewers are rarely meticulous in reading and reporting on the papers. Moreover, the security proofs themselves are usually relegated to the appendix, which reviewers are not expected to read. Journal editors as well are finding it increasingly hard to find referees of cryptography articles who are willing to spend the time to write a detailed report and evaluation. Of course, program committee members and referees themselves are also under publish-or-perish pressure. Recognition and prestige go to the authors of papers, not to their reviewers. So it is no surprise that most would rather work on their own papers than spend time wading through someone else's long, turgid, notation-laden security reductions.

Nor is it surprising that often a long time elapses between the publication of a security proof for a protocol and the discovery of an attack on the protocol that invalidates the security guarantees. For example, in 2018 practical attacks (see [191]) were discovered on the authenticated encryption scheme OCB2 that was published in 2004 [262] and standardized by ISO in 2009 [193].

In Table 1 we list some of the most notable security proofs that later were found to be flawed. They concern protocols that are or have been of practical importance, and

seven of the ten fallacious proofs were published in the prestigious Crypto and Eurocrypt conference proceedings.

The first major example of an erroneous proof for an important protocol — the error in the OAEP security proof that went unnoticed for seven years — prompted some soul-searching by researchers. In [282], Stern, Pointcheval, Malone-Lee, and Smart commented:

> Methods from provable security, developed over the last twenty years, have been recently extensively used to support emerging standards. However, the fact that proofs also need time to be validated through public discussion was somehow overlooked. This became clear when Shoup found that there was a gap in the widely believed security proof of OAEP against adaptive chosen-ciphertext attacks.... the use of provable security is more subtle than it appears, and flaws in security proofs themselves might have a devastating effect on the trustworthiness of cryptography.

According to Bellare and Rogaway [47], "In our opinion, many proofs in cryptography have become essentially unverifiable. Our field may be approaching a crisis of rigor." Halevi [173] said that "some of the reasons for this problem are social (e.g., we mostly publish in conferences rather than journals)."

Since the early 2000s when these remarks were made, quality control has not notably improved. In 2002, papers were being posted on eprint.iacr.org at the rate of fewer than four per week; in 2018 the average rate was 24 per week — a total of 1251 for the year! Some of this increase can be attributed to the increase in the number of researchers around the world who have entered the profession, some to a broadening of the field of cryptography, and some perhaps to an increase in the popularity of eprint. However, it is apparent that the number of papers has increased out of all proportion to the amount of high-quality research. Could anything be done to reduce the pressure on people to churn out papers at such a ferocious rate? For example, could academic employers and personnel committees be persuaded to put less emphasis on the sheer quantity of research publications? That seems to be an intractable task.

5.1.1. *RSA signature screening.* The flaw in the security proof in [36] for an RSA signature scheme was an essential one, since there was a simple attack. That proof implicitly assumed that all of the signed messages are distinct, although the security definition did not require that. Without that assumption, it is possible to insert an arbitrary additional (unsigned) message. Recall that a set of message-signature pairs (M_i, s_i) from a signer with RSA public key (n, e) is screened by verifying that $(\prod s_i)^e \equiv \prod h(M_i) \pmod{n}$, where h is the hash function. Suppose $e = 3$ and we replace one of the pairs (M, s) by $(M, h(M')s)$ and insert three copies of $(M', 1)$. The new set of pairs will still verify.

Although the proof in [36] is valid under a restricted definition that requires the messages to be distinct, Bellare, Nanprempre, and Neven [40] have argued (in the context of aggregate signatures) that "these restrictions preclude interesting applications, make usage of the schemes error-prone and are generally undesirable in practice."

5.1.2. *More flaws.* Fallacies have been found in proofs of security claims for a broad range of protocols. Below we list various protocols or types of protocols followed first by a reference to a paper or papers claiming provable security results and next by a reference to the paper or papers that exposed the flaws.

(1) Rabin-Williams signature scheme [223] [52].
(2) The ESIGN signature scheme [248] [282].
(3) Several Diffie-Hellman key establishment protocols [73, 195, 292, 34] [113].
(4) Fair blind signatures [5, 4] [187].
(5) Signcryption [228, 296, 229, 232] [284, 285, 286, 287].
(6) Property preserving symmetric-key encryption [250] [96].
(7) Authenticated encryption [241] [71] and [299] [270].
(8) Public-key encryption [280] [19].
(9) Public-key encryption with conjunctive keyword search [251] [190].
(10) Polly cracker public-key encryption scheme [6] [178].
(11) Unidirectional proxy re-encryption [272] [114].
(12) Sender-equivocable encryption [140] [185].
(13) Identity-based encryption [102] [8].
(14) Identity-based signatures [153] [97].
(15) Lattice-based signature scheme [21, 11] [12].
(16) Structure preserving signature scheme [176] [146].
(17) Group signature scheme [150] [192].
(18) Two-round multi-signature schemes [20, 233] [133].
(19) Lightweight identification protocol [80] [145].
(20) Key encapsulation mechanisms (KEMs) [180, 181] [57].
(21) Pseudorandom functions that resist related-key attacks [35] [3]
(22) Direct anonymous attestation (DAA) [77, 107, 106, 79, 101] [108, 105, 294, 82].

The large number of flaws pointed out in DAA security proofs is particularly noteworthy, since, as remarked in [82], "DAA is widely used in the area of trusted computing. Over 500 million TPMs have been sold, making DAA probably the most complex cryptographic scheme that is widely implemented."

5.1.3. *Flaw-spotter extraordinaire.* If the IACR some day decides to give a special award to the most prolific flaw-spotter, our nomination for this honor would be Mridul Nandi of the Indian Statistical Institute. Nandi and coauthors have found fallacies in security proofs for several types of protocols. We list some of them, followed by references first to the paper containing the original proof and then to the paper reporting on the flaw:

(1) The MAC schemes CBC-MAC and EMAC (see item (6) in Table 1), LightMAC+ [244] [227], and PMAC_TBC1k [243] [230].
(2) The symmetric encryption scheme POEx [143] [197].
(3) The authenticated encryption schemes COBRA [16] [245] and PAE [266] [92].
(4) The cipher-lengthening scheme XLS (see item (8) in Table 1).
(5) Hash functions [131] [95].
(6) Signcryption [15] [247].

In some cases — EMAC, PMAC_TBC1k, and the signcryption and hash function papers — the proof could be fixed or replaced by a correct proof of the claim. In the case of CBC-MAC the proof was fixed but with looser bounds [196]. In the case of POEx the authors later fixed the proof by defining a new and stronger notion of hash functions, but they did not give any practical instantiation of such hash functions. In some cases — LightMAC+ and COBRA — the claimed security bound was incorrect, as demonstrated

by new attacks. PAE and the XLS cipher-lengthening scheme turned out to be completely insecure. PAE was later modified [93], whereas XLS was withdrawn.

5.2. **Will a high-tech fix solve this problem?** Given the small probability of success in attacking the sociological, cultural, and psychological causes of the quality control problem, it is natural to look for a high-tech fix. After all, computers have so often come to rescue us from the consequences of warped incentives and human laziness, carelessness, and incompetence. We've seen how computers have reversed the decline of K-12 education in America, online instruction has turned undergraduates into hard-working and creative learners, the information superhighway has reduced inequality between the rich and poor and between the Global North and Global South, smart appliances will solve the energy problem and bring global warming to a halt, and social media and the internet have strengthened American democracy and prevented the election of demagogues, liars, and bigots. By the same token it stands to reason that computer-generated proofs will remove human error from provable security papers. At least that's how it looked twelve years ago when the first author wrote the first of two papers [207, 208] critiquing automated theorem-proving.

The idea that parts of mathematics can and should be mechanized goes back at least to Leibniz [283], whose most lasting contribution was to develop an approach to calculus that allows derivatives and many integrals to be computed by rote without thinking, and in our day makes it easy to code those techniques into calculators. However, in mathematics proper the role of computers in proving theorems has been very modest.

5.2.1. *Full Domain Hash (FDH).* The paper [207] analyzed in detail the claim at Crypto 2006 [61] that an automated theorem-prover had reconstructed essentially the security reduction of Bellare-Rogaway [45] for the FDH signature scheme. This seemed to be a striking achievement. The original proof of Bellare-Rogaway appeared in their seminal paper on random oracles, and FDH is arguably the simplest and most basic public key signature scheme there is. The claim in [61] seemed to give reason to hope for rapid progress in replacing tedious human work on provable security with flawless computer-generated security reductions.

Let $f : S \longrightarrow S$ be a trapdoor one-way permutation, and let h be a hash function whose values range uniformly over S; in [45] h is modeled by a random oracle. A signer Alice possesses a secret key that allows her to calculate f^{-1}; her signature on a message m is $s = f^{-1}(h(m))$. Bob can verify Alice's signature by checking that $f(s) = h(m)$. It's as simple as that.

The security reduction in [45] showed that an adversary who makes up to q_h hash queries and q_s signature queries and takes time t to forge a signature for a message of the adversary's choice can then be used to invert f (that is, find x such that $f(x) = y$ for given $y \in S$) in time of order tq_h. In the case of FDH-RSA, Coron [116] reduced this time to tq_s.

Although the paper [61] gives the impression that it is essentially automating the proof in [45], a careful comparison [207] revealed that the computer-generated proof in [61] is far less satisfactory than the human proof in [45] for several reasons:

(1) The computer-generated "proof" does not give a reduction at all, but rather just formalizes an intuitive argument of the sort that most theoreticians regard as merely "heuristic." Interaction is not simulated.

(2) The factor q_h in the adversary's probability of success comes not from the interaction but rather from the possibility that f^{-1} is not uniformly hard to compute over S.
(3) In the case of FDH-RSA it is unclear whether the theorem-prover can be modified to give Coron's improvement.
(4) The probability space used in the proof is not the appropriate one in a situation where there is a non-negligible subset of weak keys.
(5) The theorem-prover used 14800 lines of Ocaml code.

5.2.2. *Recent work.* Since the publication of [207] and [208], a significant amount of work has been done on automatic proof verification and automatic proof generation for cryptographic protocols; for representative examples, see [13, 14, 23, 24]. It remains to be seen whether these techniques yield proofs that require less human effort and are more reliable than well-written human-generated proofs, and whether automated theorem proving tools will be widely adopted by cryptographers.

Work by Bhargavan *et al.* on the provable security of TLS 1.2 [59] and TLS 1.3 [58] has received much attention. The paper [59] reports on a reference implementation of TLS 1.2 comprising approximately 5,000 lines of code in the F♯ programming language that is machine verified using the 'F7 typechecker.' This work is notable since TLS is a complicated protocol with many versions, options, and important implementation details that are usually neglected in human-generated security proofs (as we saw in §3.2). As mentioned in [59], the security proofs obtained have some limitations — they do not account for timing attacks, the reference code is not optimized for performance, some algorithms and ciphersuites are not supported, and concrete security bounds are not derived.

The paper [58] reports on the first (semi-automated) machine-checked cryptographic proof for TLS 1.3, which was done using the verification tool CryptoVerif. The security proof has some limitations; for example, it does not consider downgrade attacks. However, it does claim security for the "pre-shared key" (PSK) option in TLS 1.3, wherein the client and server use a shared secret key in the handshake protocol that was either generated using an earlier handshake or was distributed out-of-band. In addition to the analysis in [58], automated symbolic analysis of the PSK option in TLS 1.3 was presented in [127], and hand-generated proofs for the PSK handshake protocol were given in [141]. It thus came as a surprise when in March 2019 Drucker and Gueron [134] discovered a 'reflection attack' on the PSK handshake protocol in TLS 1.3. This is a type of intruder-in-the-middle attack in which a client is led to false beliefs about the identity of the party it's communicating with. Drucker and Gueron explain the gaps in the TLS 1.3 analysis in [127] and [141] and remark:

> Proofs that are produced by automatic tools may be incorrect or incomplete if the underlying model does not capture all the assumptions or if its details are not fed correctly.

5.3. **Non-constructible algorithms.** A *non-uniform* algorithm differs from Turing's notion of an algorithm in that for each input length k it's permitted to have an "advice string" of length bounded by a polynomial in k that might help solve the problem. Because the term "non-uniform" is sometimes used in the cryptographic literature in a broader sense that's inconsistent with its technical meaning — for example, when the advice strings do not depend only on the input length — in this section we shall often use

the informal term "non-constructible" rather than "non-uniform." A non-constructible algorithm typically makes use of an advice string that exists mathematically but in practice is infeasible to find.

There is a widespread opinion among cryptographic researchers — a viewpoint that we devoted much of [216] to refuting — that the non-uniform model of complexity is the appropriate one for security proofs. In an email [27] to the first author responding to our critique of [26], Bellare wrote:

> My paper uses a concrete complexity framework. Such a framework is inherently non-uniform. This has been understood since such frameworks started.... [W]hen complexity is concrete, we have non-uniformity.... I had no idea my paper would be read by anyone not familiar with the fact that concrete security is non-uniform.

According to Coretti, Dodis, Guo, and Steinberger [115],

> Hence, by and large it is believed by the theoretical community that *non-uniformity is the right cryptographic modeling of attackers,* despite being overly conservative and including potentially unrealistic attackers. (emphasis in original)

This belief in the superiority of non-uniform complexity for cryptography is often explained by saying that a theorem proved in the non-uniform model of complexity is stronger than if it were proved in the standard uniform model. In their lecture notes for a course at MIT [163], Bellare and Goldwasser state:

> Clearly, the non-uniform adversary is stronger than the uniform one. Thus, to prove that "something" is "secure" even in presence of a non-uniform adversary is a better result than only proving it is secure in presence of a uniform adversary. (p. 254)

Suppose that a provable security reduction takes the form $\mathcal{P} \longrightarrow \mathcal{Q}$, or, equivalently, not-$\mathcal{Q}$ $\longrightarrow$not-$\mathcal{P}$, where $\mathcal{P}$ is an efficient algorithm for the adversary's task and $\mathcal{Q}$ is an efficient algorithm to solve a problem that is believed to be hard. If the proof is in the non-uniform model, then the conclusion not-$\mathcal{P}$ is stronger than in the uniform model: even a non-uniform adversary is unable to break the protocol. The fallacy in the viewpoint expressed above is that the hypothesis of the theorem — that is, not-$\mathcal{Q}$ — is also stronger, because it says that the problem cannot be efficiently solved even by a non-uniform algorithm. If both the hypothesis and the conclusion of a non-uniform theorem are stronger than those of a uniform theorem, then the two theorems are not comparable — neither is stronger than the other.

Cryptographers who claim that non-uniform theorems are stronger because their conclusions are stronger are forgetting that the hypotheses also become stronger, that is, they cannot point to the underlying problem's resistance to uniform algorithms as evidence for the hypothesis. It's usually unclear how to test the hypothesis of a non-uniform theorem. Real-world algorithms do not have advice strings that are exponentially difficult to find. If the hypothesis is essentially untestable, then the theorem is not of much value.

For example, in [155] Garg and Gupta presented a blind signature scheme and proved its blindness property under the assumption that a variant of the discrete logarithm problem is intractable even against non-uniform attacks. However, when selecting concrete parameters for the blind signature scheme, the authors only accounted for the known

uniform attacks on the discrete logarithm problem. In [281] Soundararajan described a non-uniform attack on the discrete logarithm problem and investigated its effect on concrete parameters for the scheme in [155].

We next recall the most important case when a leading cryptographer was led astray by ignoring the need to test the hypothesis against non-uniform algorithms. This occurred at Crypto 2006 [26] (see also [28]).

5.3.1. *The HMAC message authentication code.* HMAC [32, 33] is a popular hash-function-based message authentication code (MAC). The main result in [26] concerns NMAC, a closely related MAC. We shall summarize the security theorem and the flawed interpretation in [26] in a slightly simplified form; for more details, see [215, 218] and §§4-5 of [99].

By a compression function we mean a function $z = f(x, y)$, where $y \in \{0,1\}^b$ and $x, z \in \{0,1\}^c$; typically $b = 512$ and c is equal to either 128 (for MD5), 160 (for SHA1), or 256 (for SHA256). Given a compression function f, to construct an iterated hash function h one starts with an initialization vector IV, which is a publicly known bitstring of length c that is fixed once and for all. Suppose that $m = (m_1, ..., m_r)$ is a message consisting of r blocks. We set $x_0 = \text{IV}$, and for $i = 1, ..., r$ we recursively set $x_i = f(x_{i-1}, m_i)$; finally, we set $h(m) = h_{\text{IV}}(m) = x_r$, which is the c-bit hash value of m.

Suppose that Alice shares two secret c-bit keys k_1 and k_2 with Bob, and wants to create an NMAC-tag of a message m so that Bob can verify that the message came from Alice. She first uses k_1 as the IV and computes $h_{k_1}(m)$. She pads this with $b - c$ zeros (denoted by a 0-superscript) and sets her tag $t(m)$ equal to $h_{k_2}(h_{k_1}(m)^0)$.

The purpose of finding a security reduction for NMAC is to show that if one has confidence that the compression function f enjoys a certain security property, then one can be sure that NMAC has the same property. Two decades ago HMAC was first proposed by Bellare, Canetti, and Krawczyk [32, 33]. In [32] they proved (assuming weak collision-resistance of h) that if f has the secure-MAC property (a type of unforgeability), then so does NMAC. The proof in [32] was tight, short, and easy to read.

In 2006 Bellare [26] published a different security reduction for NMAC. First, he dispensed with the collision-resistance assumption on h, which is a relatively strong assumption that has turned out to be incorrect for some real-world iterated hash functions. Second, he replaced the secure-MAC property with the stronger pseudorandom-function (PRF) property, that is, he showed that if $f(x, y)$ (with x serving as the hidden key) has the PRF property, then so does NMAC. The PRF property says that the function with hidden key is essentially indistinguishable from a random function. This was important in order to justify the use of HMAC for purposes other than message authentication — in applications where the PRF property is desired, such as key-derivation protocols and password systems.

However, in 2012 we found a flaw in [26]. For Bellare, who along with Rogaway popularized the concept of "practice-oriented provable security" [25], it was important to determine in real-world terms what guarantee his theorem provided. To do this, Bellare's approach was to take the fastest known generic attack on the PRF property of a compression function, and evaluate what his theorem then implied for the security of NMAC. In his analysis he took the key-guessing attack as the best generic attack on f, and concluded that NMAC is secure "up to roughly $2^{c/2}/r$ queries." For instance, for $r \leq 2^{20}$ Bellare

was claiming that NMAC-MD5 is secure up to 2^{44} queries and NMAC-SHA1 up to 2^{60} queries. (In 2006, MD5 and SHA1 were common choices for hash functions.)

Bellare failed to account for the fact that his security reduction was carried out by means of a non-constructible algorithm — namely, it used an advice string consisting of a pair of messages that maximized a certain probability. Because of this, he was logically required to examine security of f against non-constructible algorithms, not just uniform attacks. There are simple generic non-constructible algorithms that attack the PRF property and have a much higher success probability than the key-guessing attack. For example, let y_0 be an element of $\{0,1\}^b$ for which the 5th bit of $f(x,y)$ has the highest probability, taken over all $x \in \{0,1\}^c$, of being 1. Given a function that is either a random function $R(y)$ or $f(x,y)$ with a random hidden key x, one can get a significant advantage in guessing whether it's $R(.)$ or $f(x,.)$ by asking for its value at y_0 and guessing the former if the 5th bit of output is 0 and the latter if it's 1. This is a non-constructible algorithm because one uses the advice string y_0, which would be infeasible to compute if it weren't given to you.

If one repeats Bellare's analysis using this type of non-uniform attack, one finds that NMAC's security is guaranteed only up to at most $2^{c/4}/\sqrt{r}$ queries, that is, 2^{22} for NMAC-MD5 and 2^{30} for NMAC-SHA1. That level of security is of little value in practice. There might well be much faster non-uniform attacks on the prf property for the compression function of a particular hash function. So even the 2^{22} and 2^{30} guarantees for NMAC-MD5 and NMAC-SHA1 are very optimistic.

5.4. **Tightness.** A security reduction for a protocol typically has the following form: A certain mathematical task $\mathcal{Q}$ reduces to the task $\mathcal{P}$ of successfully mounting a certain type of attack on the protocol — that is, of being a successful adversary in a certain security model. More precisely, the security reduction is an algorithm $\mathcal{R}$ for solving the mathematical problem $\mathcal{Q}$ that has access to a hypothetical oracle for $\mathcal{P}$. If the oracle takes time at most T and is successful with probability at least ε (here T and ε are functions of the security parameter k), then $\mathcal{R}$ solves $\mathcal{Q}$ in time at most T' with probability at least ε' (these are again functions of k). The *tightness gap* is the ratio $T'\varepsilon/T\varepsilon'$. We say that $\mathcal{R}$ is a *tight* reduction if this gap is small. But if the tightness gap is 2^{40}, then one is guaranteed only that the adversary's task is at least 2^{-40} times as hard as solving the supposedly hard problem $\mathcal{Q}$.

How should we interpret a large tightness gap? What does it mean for the real-world security of the protocol? The possibilities are essentially the same as for flaws in a proof (see §5.1), namely:

(1) A different proof with a much smaller tightness gap (or none at all) can be found. Perhaps a small modification in the original protocol can be made that makes it possible to give a tight proof.
(2) A tight proof can be given if we make stronger assumptions. If we're lucky, the need for stronger assumptions will be mainly of theoretical interest and will not cause security concerns for practical implementations.
(3) No tight reductionist proof can be found, but there's a really convincing heuristic argument that in practice seems to imply that we needn't increase parameter sizes to account for the tightness gap.

(4) The non-tightness reflects the real-world security of the protocol. That is, there is an attack that shows that the protocol is insecure if parameter sizes are used that would have given a secure protocol had the proof been tight.

As in the case of fallacious proofs, the last possibility is a "nightmare scenario" [238]. Until it is ruled out — for example, by finding a different security reduction that is tight — a large tightness gap in a proof should never be dismissed as a minor issue.

5.4.1. *Pseudorandom bits and stream ciphers.* An asymptotic big-O estimate can easily hide a large tightness gap that renders the estimate useless in the practical range of parameters. In [209] we looked at both asymptotic and concrete security estimates for the factorization-based Blum-Blum-Shub pseudorandom bit generator [62]. The asymptotic estimate in [290, 9] showed that one can securely extract $O(\log\log n)$ bits from each squaring mod n. This was interpreted (see [136, 297]) as meaning that if we have a 768-bit RSA modulus n, then we can securely extract 9 bits in each iteration, since $9 < \log_2\log_2(n)$.

However, if one uses the best available concrete results, which were obtained in [277, 9], one finds that with a 768-bit modulus the extraction of 9 bits in each iteration is secure against an adversary whose time is bounded by a huge *negative* number in the case of [277] and by 2 to a large *negative* power in the case of [9]!

In [48] (see also [49]) a stream cipher QUAD was proposed. It was supported by a non-tight reductionist security proof, based on the NP-hard problem MQ of solving a system of multivariate quadratic polynomial equations over a finite field. In [295] Yang *et al.* demonstrated attacks on three QUAD parameter sets for which timings had been given at the Eurocrypt 2006 talk that accompanied [48]. The stream cipher was broken for one parameter set; the underlying MQ problem was broken for the second parameter set; and the security proof was shown to provide no guarantees for the third parameter set. These attacks highlight the dangers in relying on non-tight reductionist proofs based on problems whose concrete hardness is not well understood.

5.4.2. *The multi-user setting.* As remarked in §3.7, just because a system enjoys an acceptable level of security in the single-user setting it does not follow that the same is true when it is deployed in practice in the multi-user setting, where an adversary's goal might be to compromise any one of n users.

In [100] the authors demonstrate attacks on some encryption schemes in the multi-user setting that are n times faster than the fastest known attacks in the single-user setting, where n is the number of users. Among these schemes are the Synthetic Initialization Vector (SIV) deterministic authenticated encryption scheme [264], the Offset Codebook (OCB) mode authenticated encryption scheme [263], and the ECB-mask-ECB (EME) disk encryption scheme [175]. These schemes all have proofs of security in the single-user setting, and the attacks show that extending the proofs to the multi-user setting inevitably results in a tightness gap of n. In [99] the authors highlight multi-user attacks by Zaverucha [298] on some standardized hybrid encryption schemes (such as [276]).

In [100] a natural reduction was described from the problem of breaking a message authentication code (MAC) in the single-user setting to the problem of breaking the scheme in the multi-user setting. The tightness gap in the reduction is n, the number of users. An attack on the MAC scheme in the multi-user setting was presented that was n times faster than the fastest generic attack on the MAC scheme in the single-user setting.

Similar attacks were also mounted on some other protocols with non-tight reductionist security proofs in the multi-user setting, including a network authentication protocol [86], an aggregate MAC scheme [203], a hierarchical in-network data aggregation scheme [94], and a history-free aggregate MAC scheme [137].

Considerable work has been done in recent years on designing cryptographic protocols that have reductionist security proofs in the multi-user setting whose tightness gaps do not (significantly) depend on the number of users. Examples include MAC schemes [29], signature schemes [204], aggregate signature schemes [224], Galois counter mode (GCM) in authenticated encryption [231], hybrid encryption [160], and key agreement [18].

If one wants to base confidence in a protocol on a non-tight security reduction, one cannot use parameters that would give the desired level of security had the reduction been tight. But in general standards bodies do not take into account tightness gaps when recommending parameter sizes, as we saw in §5.4.1 in the case of Blum-Blum-Shub pseudorandom bits. An apparent exception to this was an Internet Engineering Task Force (IETF) debate over whether or not to require that the public key be included in the input to the hash function in its standard for Schnorr signatures [267]. The issue was whether or not security for such signatures is equivalent in the single-user and multi-user settings — a question that has had a somewhat confusing history. In [151] Galbraith, Malone-Lee, and Smart gave a tight reduction from an adversary in the single-user setting to an adversary in the multi-user setting, with no need to include public keys in the hash. Thirteen years later, Bernstein [53] found a flaw in their proof, and also proved that a tight security reduction could be restored if the public key is included in the hash function. In response to Bernstein's results, the IETF decided to mandate inclusion of the public key. Later Kiltz, Masny, and Pan [204] gave a tight security reduction without needing to include the public key in the hash function; however, their assumptions are stronger than in [151]. What is peculiar about all this is that the known security reductions for Schnorr signatures in the single-user setting are highly non-tight[1]. Even if the tightness gap remains between single-user and multi-user settings, this is only a small part of the tightness problem for Schnorr signatures.

5.4.3. *Existential vs universal private key recovery.* In the multi-user setting the difference between existential and universal key recovery is that in the former case the adversary is deemed successful if she captures any user's private key, whereas in the latter case she needs to be able to attack an arbitrary user that's given to her in advance. If provable security is a priority, then we will want to be able to give a tight proof of equivalence between existential and universal adversaries. In §5.3 of [209] we discussed the questionable conclusion this leads to concerning parameter selection for ECC encryption. If each user selects a different elliptic curve, then no tight reduction from universal to existential key recovery is known; but if all users work with a fixed curve, then it is not hard to give such a reduction. Yet it defies common sense to think that real-world security of private keys is greater when a system-wide elliptic curve is fixed than when the choice of curve varies. In [209] we comment, "On the contrary, what this example shows is that it is sometimes

[1]An exception is the tight proof of Schnorr-Jakobsson [268], which, however, requires both the random oracle and generic group assumptions, both of which are very strong. The use of the generic group model, in particular, is regarded as leading to weak assurances; see §4.2.2.

foolish to use the existence or absence of a tight reductionist security argument as a guide to determine which version of a cryptosystem is preferable."

5.4.4. *WOTS-PRF.* In [81], a variant of the Winternitz one-time signature (WOTS) scheme that uses a pseudorandom function (PRF) $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ was proposed. The tightness gap of the security proof in [81] has a factor κ^{w-1}, where w is the "Winternitz parameter" (e.g., $w = 64$), and κ is the size of the largest subset K of $\{0,1\}^n$ for which there exist $x, y \in \{0,1\}^n$ with $f(k,x) = y$ for all $k \in K$.

In [81] it was claimed that if f has the PRF property, then $\kappa \leq 2$. However, it was observed in [225] that the argument given for this claim is non-constructible. Namely, if $\kappa > 2$ then there must *exist* $x, y \in \{0,1\}^n$ for which $f(k,x) = y$ for κ keys $k \in \{0,1\}^n$, and in [81] it is shown that such a pair (x,y) can be used to construct an algorithm that supposedly violates the PRF property of f. Now, since no efficient method is known for finding the pair (x,y), what is described in [81] is actually a non-constructible attack on the PRF property of f. But in the argument the authors use an assessment of the security of f based on the known *constructible* attacks on the PRF property. Thus, the argument fails to support the claim that $\kappa \leq 2$.

In fact, it is shown in [225] that the opposite is true: for a *random* function the expectation is that $\kappa \geq \ln(2^n)/\ln\ln(2^n)$. This means that if the claim in [81] were true, a random function would fail the PRF property, which is absurd. If we perform a concrete analysis of probabilities in the case $n = 256$, we find that the expected value of κ is 98, and so with $w = 64$ the tightness gap in the security proof in [81] has a factor κ^{w-1} approximately equal to 2^{416}, which is much larger than the factor 2^{63} claimed in [81]. Thus, the security proof in [81] provides little or no security guarantee for the WOTS-PRF signature scheme.

5.4.5. *XMSS-T.* In [188] Hülsing, Rijnveld, and Song proposed a hash-based signature scheme XMSS-T with a tight security proof. Peikert [254] observed that their security proof makes an assumption that is almost certainly false in practice, namely, that a pseudorandom function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ satisfies the following property: for each $k \in \{0,1\}^n$, there is no $y \in \{0,1\}^n$ that has exactly one preimage under the function $g_k : \{0,1\}^n \to \{0,1\}^n$ defined by $g_k(x) = f(k,x)$. (The authors of [188] wrote, "Please note that this requirement meets the expectation for a random function.") A simple probabilistic argument shows that for a random function from $\{0,1\}^n$ to $\{0,1\}^n$ the expectation is that $1/e \approx 37\%$ of the elements of $\{0,1\}^n$ have exactly one preimage, and thus there is negligible probability that the function f satisfies the property assumed in [188]. (Note the similarity with the error in [81] discussed in §5.4.4 above.) Peikert also observed that the security proof in [188] can be easily patched, but at the expense of a significant increase (e.g., 2^{60}) in the reduction's tightness gap.

What is troubling about the flawed security reduction in [188] is that XMSS-T is used in the SPHINCS+ signature scheme [54], which is a proposed quantum-safe protocol currently being considered by NIST. As a result, the security theorem for SPHINCS+ (Theorem 9.1 in [54]) also understates the tightness gap[2]. This is an example of how a flaw in a security proof can propagate to other papers whose authors use the result without being aware of the problem with the proof.

[2]This shortcoming has been addressed in [55].

5.4.6. *Lattice-based cryptography.* Among the various proposals for quantum-safe public key cryptosystems, the lattice-based schemes are promoted as having a unique security feature that the competitors lack, namely, a rigorous proof giving a reduction to the *average* case of the underlying mathematical problem from the *hardest* case of a (different) problem that is believed to be hard. This claim was examined in [99] and was found to be problematic for several reasons. Here we give only a brief summary; for details see §6 and Appendix A of [99].

The underlying mathematical problem is Learning With Errors (LWE), which is a linear algebra problem in which the vector on the right is given with a certain error according to a specified distribution. A theorem of Regev [260] relates the average case of Decision LWE to the hardest case of the γ-approximate Shortest Independent Vector Problem (SIVP_γ). Let L be an n-dimensional lattice defined by some basis of integer vectors. Then SIVP_γ is the problem of finding a basis whose longest vector is within a factor of γ of being optimal (that is, its length is no greater than γ times the length of the longest vector in a basis where this length is minimal). For small γ, SIVP_γ is known to be NP-hard.

First of all, Regev's theorem and essentially all work on average-case/hardest-case reductions of lattice problems are asymptotic and lack any practice-oriented analysis in terms of concrete parameter values. In [99] the authors give a concrete analysis for certain reasonable parameter values and find a tightness gap of 2^{504} in that case. That is, "if average-case DLWE can be solved in time T, then [Regev's] Theorem 1 shows that SIVP_γ can be solved by a quantum algorithm in time $2^{504}T$."

In the second place, the hardness of SIVP_γ for the relevant values of γ has not been seriously studied. It is known only that for much smaller γ the problem is hard and for much larger γ it is easy. In the third place, there are additional tightness gaps in the reductions that relate the adversary's task in attacking the protocols to the LWE problem.

In [253] Peikert describes asymptotic analyses of the security of lattice-based systems, and concludes:

> ...worst-case reductions give a hard-and-fast guarantee that the cryptosystem is at least as hard to break as the hardest instances of some underlying problem. This gives a true lower bound on security, and prevents the kind of unexpected weaknesses that have so often been exposed in schemes that lack such reductions.

In [99] we comment:

> This would be true in a meaningful sense if the reductions were tight and if the underlying problem were SIVP_γ for a small γ (small enough so that SIVP_γ is NP-hard or so that there is reason to have confidence that there are no efficient algorithms for SIVP_γ). However, neither is the case. When discussing asymptotic results and writing for a broad readership interested in practical cryptography, the use of such terms as "hard-and-fast guarantee" and "true lower bound on security" is inappropriate and misleading, because in real-world cryptography the normal interpretation of these terms is that one has concrete practical security assurances.

6. Errata

1. In a historical digression in [210] we discussed the absence of a security reduction for the discrete-log-based Digital Signature Algorithm (DSA) that the NSA proposed and that was strenuously opposed by supporters of RSA signatures. We wrote:

> It is also surprising that apparently none of the NSA cryptographers noticed this possible objection to DSA [i.e., absence of a security proof]; if they had, they could have easily fixed it (without any significant loss of efficiency) by having the signer evaluate the hash function at (m, r) rather than just at m.

This is incorrect. In order to make a Schnorr-type proof go through one would need to include $r = (g^k \bmod p)$ in the signature rather than $r = ((g^k \bmod p) \bmod q)$. Here p and q are primes such that $q \mid (p-1)$ and the bitlength of p is several times the bitlength of q, g is a generator of the order-q subgroup of $\mathbb{Z}_p^*$, and k is a random exponent. Thus, to get a proof DSA would have had to have been modified so as to have much longer signatures. It's no surprise that this wasn't done: when DSA was proposed more than a quarter century ago, inefficiency was a deal-breaker, but absence of a reductionist security proof was not.

2. In [213] and [214], in discussing a protocol proposed in [66], we confused two different constructions from that paper — ordered multi-signatures (OMS) and identity-based sequential aggregate signatures (IBSAS). We should have referred to the paper's IBSAS construction rather than to the OMS construction. A sequential aggregate signature is a single compact signature produced by several people acting sequentially. It has fixed length independent of the number of signers, and the signers may be signing different messages. The main application discussed in [66] is to secure routing of messages through a network.

3. Some readers have pointed out that part of the conclusion of [207] was poorly written, in the sense that the purpose of the paragraph was obscure. Especially troubling is the possibility that a reader might not catch the sarcasm:

> One of the great insights of post-modernism [279] is that there is no such thing as scientific progress, and one should not speak of one approach being better or worse than a different one. Science, like other areas of human endeavor, is subjective and culturally determined, according to those who view the history of science as a more or less arbitrary sequence of shifts from one paradigm to another. Thus, if we want to adhere to the tenets of post-modern cryptography (a term that Oded Goldreich [162] obligingly introduced into common use), we should embrace all possible approaches to "proving" security of cryptographic protocols and should resist the temptation to call game-hopping and automated theorem-proving a step backward.

For the record, we are not post-modernists, we are not opposed to scientific progress, and we do not believe that scientific progress does not exist. Goldreich's claim to the contrary in [162] is incorrect.

7. Conclusion

Norbert Wiener once said (quoted in [130]):

> One of the chief duties of the mathematician in acting as an advisor to scientists...is to discourage them from expecting too much from mathematics.

The "another look" series of papers can all be found at http://anotherlook.ca. The "Overview" page of that site summarizes our viewpoint as follows:

> We wish to emphasize that we are not opposed to proofs in cryptography. Mathematical proofs have their place. What we are opposed to is the misleading hype that often accompanies them. We believe that designers of protocols would be on more solid ground if they (1) deleted the terms "proof of security" and "provable security" from the cryptographic lexicon, and (2) showed some humility and realism when presenting security assurances to the public.
>
> Above all, our work highlights the important role that old-fashioned cryptanalysis and sound engineering practices continue to play in establishing and maintaining confidence in the security of a cryptographic system.

Two decades ago Victor Shoup [274] expressed a bold confidence, widely held at the time, in reductionist security proofs:

> If we can prove security in this way, then we essentially rule out all possible shortcuts, even ones *we have not yet even imagined*. The only way to attack the cryptosystem is a full-frontal attack on the underlying hard problem. Period. (p. 15; emphasis in original)

History has proved him wrong — again and again.

In their article surveying the "science of security," Herley and van Oorschot [177] dispute the notion that formal security reductions should be favored over empirical analysis:

> ...while it is correct to note that empirical evidence can never demonstrate the infeasibility of attacks, we must also note that the same is true of formal reasoning. The conclusion that formal approaches enjoy an inherent superiority in this respect is unsound. A proof can deliver guarantees only about a mathematical system, not a real-world one. Since it is real-world systems that we ultimately use, the choice is not between one approach which offers immunity to attack and another which does not. Rather, the question is to what degree properties proven about a mathematical system can be translated into useful properties of a real-world one. Speaking of mathematical and real-world systems in the same argument and suggesting that the properties proved of one are naturally enjoyed by the other is a recurring error.

In the same vein, in their overview of the provable security field [129], Degabriele, Paterson, and Watson explain the reason for skepticism among practitioners:

> Provable security has become an important research area in modern cryptography but is still met with skepticism by many in the practical community. This is understandable considering the types of attack that we outline here. Practitioners might think provable security results provide an absolute statement of security, especially if they're presented in such a

manner. When they later discover that a scheme is insecure because of an attack outside the security model, this might damage their confidence in the whole enterprise of provable security.

* * *

There can be dangers as well as benefits when mathematical methods become dominant in the study of questions that have a large human component. In the middle of the last century Darrell Huff [186] wrote entertainingly of the myriad ways that commercial and political advertisers use statistics to mislead the public. In our time David Freedman [144] has written about the unreliability of quantitative studies in medicine; Felix Salmon [265] has described how David Li's mathematical model for collateralized debt obligations was seized upon by Wall Street as a justification for irresponsible investment practices that precipitated the financial crisis of 2008; and Cathy O'Neil [249] has explained many of the ways that data science has been used to undermine democratic values — for example, by reinstituting a type of racial discrimination in lending (called "redlining") that had supposedly been outlawed in the U.S. fifty years ago.

As we discussed in [205], cryptography exists in a very different realm from mathematics; its development depends on historical, political, cultural, and economic contingencies. If we ever meet an advanced extraterrestrial species, they will undoubtedly know about perfect circles, right triangles, modular curves, and differential equations — the Platonic Ideals of mathematics, in the terminology of the ancient Greeks. But they will not be using AES, SHA256, or ECDSA.

It is in part the element of human interaction, of "spy vs spy" that makes cryptography an exciting field of study. The history of cryptography, including its most recent history, is dramatic precisely because it is so often unpredictable, with the best-laid plans of "scientific" cryptographers failing miserably when real-world implementations confront real-world adversaries. This is nothing to be ashamed of. We should not envy pure mathematicians because their perfect circles or modular curves do not bite them back or because their theorems are 100% unconditionally valid and ours are not. Cryptography is as much an art as a science, and it's time to make peace with that fact.

Acknowledgments

We wish to thank Dan Bernstein, Ian Blake, Sanjit Chatterjee, Sam Jaques, Paul van Oorschot, Francisco Rodríguez Henríquez, and Palash Sarkar for helpful comments on an earlier draft; and Ann Hibner Koblitz for editorial corrections and comments. Needless to say, all the opinions expressed in this article are the sole responsibility of the authors.

References

[1] M. Abdalla *et al.*, Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions, *J. Cryptology*, **21** (2008), pp. 350-391.

[2] M. Abdalla, M. Bellare, and G. Neven, Robust encryption, *Theory of Cryptography Conference — TCC 2010*, LNCS 5978, pp. 480-497.

[3] M. Abdalla, F. Benhamouda, A. Passelègue, and K. Paterson, Related-key security for pseudorandom functions beyond the linear barrier, *Advances in Cryptology — Crypto 2014*, LNCS 8616, pp. 77-94.

[4] M. Abe, A three-move blind signature scheme for polynomially many signatures, *Advances in Cryptology — Eurocrypt 2001*, LNCS 2045, pp. 136-151.

[5] M. Abe and M. Ohkub, Provably secure fair blind signatures with tight revocation, *Advances in Cryptology — Asiacrypt 2001*, LNCS 2248, pp. 583-601.
[6] M. Albrecht, P. Farshim, J. Faugère, and L. Perret, Polly cracker, revisited, *Advances in Cryptology — Asiacrypt 2011*, LNCS 7073, pp. 179-196.
[7] M. Albrecht, J. Faugère, R. Fitzpatrick, L. Perret, Y. Todo, and K. Xagawa, Practical cryptanalysis of a public-key encryption scheme based on new multivariate quadratic assumptions, *Public Key Cryptography — PKC 2014*, LNCS 8383, pp. 446-464.
[8] M. Albrecht and K. Paterson, Breaking an identity-based encryption scheme based on DHIES, *Cryptography and Coding — IMACC 2011*, LNCS 7089, pp. 344-355.
[9] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr, RSA and Rabin functions: Certain parts are as hard as the whole, *SIAM J. Computing*, **17** (1988), pp. 194-209.
[10] N. AlFardan and K. Paterson, Lucky thirteen: Breaking the TLS and DTLS record protocols, *Proc. 2013 IEEE Symposium on Security and Privacy*, pp. 526-540.
[11] E. Alkim, N. Bindel, J. Buchmann, and Ö. Dagdelen, TESLA: Tightly-secure efficient signatures from standard lattices, version 20150730:095248, available at http://eprint.iacr.org/2015/755.
[12] E. Alkim, N. Bindel, J. Buchmann, Ö. Dagdelen, E. Eaton, G. Gutoski, J. Krämer, and F. Pawlega, Revisiting TESLA in the quantum random oracle model, *Post-Quantum Cryptography — PQCrypto 2017*, LNCS 10346, pp. 143-162.
[13] M. Ambrona, G. Barthe, R. Gay, and H. Wee, Attribute-based encryption in the generic group model: Automated proofs and new constructions, *Proc. 2017 ACM SIGSAC Conference on Computer and Communications Security — CCS '17*, pp. 647-664.
[14] M. Ambrona, G. Barthe, and B. Schmidt, Automated unbounded analysis of cryptographic constructions in the generic group model, *Advances in Cryptology — Eurocrypt 2016*, LNCS 9666, pp. 822-851.
[15] J. An, Y. Dodis, and T. Rabin, On the security of joint signature and encryption, *Advances in Cryptology — Eurocrypt 2002*, LNCS 2332, pp. 83-107.
[16] E. Andreeva, A. Luykx, B. Mennink, and K. Yasuda, COBRA: A parallelizable authenticated online cipher without block cipher inverse, *Fast Software Encryption — FSE 2014*, LNCS 8540, pp. 187-204.
[17] M. Backes and D. Hofheinz, How to break and repair a universally composable signature functionality, *Information Security — ISC 2004*, LNCS 3225, pp. 61-72.
[18] C. Bader, D. Hofheinz, T. Jager, E. Kiltz, and Y. Li, Tightly-secure authenticated key exchange, *Theory of Cryptography Conference — TCC 2015*, LNCS 9014, pp. 629-658.
[19] J. Baek and Y. Zheng, Zheng and Seberry's public key encryption scheme revisited, *International Journal of Information Security*, **2** (2003), pp. 37-44.
[20] A. Bagherzandi, J. Cheon, and S. Jarecki, Multisignatures secure under the discrete logarithm assumption and a generalized forking lemma, *Proc. Fifteenth ACM Conference on Computer and Communications Security — CCS '08*, pp. 449-458.
[21] S. Bai and S. Galbraith, An improved compression technique for signatures based on learning with errors, *Topics in Cryptology — CT-RSA 2014*, LNCS 8366, pp. 28-47.
[22] E. Bangerter, J. Camenisch, and U. Maurer, Efficient proofs of knowledge of discrete logarithms and representations in groups with hidden order, *Public Key Cryptography — PKC 2005*, LNCS 3386, pp. 154-171.
[23] G. Barthe, J. Crespo, B. Grégoire, C. Kunz, Y. Lakhnech, B. Schmidt, and S. Zanella-Béguelin, Fully automated analysis of padding-based encryption in the computational model, *Proc. 2013 ACM SIGSAC Conference on Computer and Communications Security — CCS '13*, pp. 1247-1260.
[24] G. Barthe, X. Fan, J. Gancher, B. Grégoire, C. Jacomme, and E. Shi, Symbolic proofs for lattice-based cryptography, *Proc. 2018 ACM SIGSAC Conference on Computer and Communications Security — CCS '18*, pp. 538-555.
[25] M. Bellare, Practice-oriented provable-security, *Proc. First International Workshop on Information Security — ISW 1997*, LNCS 1396, pp. 221-231.
[26] M. Bellare, New proofs for NMAC and HMAC: Security without collision-resistance, *Advances in Cryptology — Crypto 2006*, LNCS 4117, pp. 602-619.
[27] M. Bellare, email to N. Koblitz, 24 February 2012.

[28] M. Bellare, New proofs for NMAC and HMAC: Security without collision-resistance, *J. Cryptology*, **28** (2015), pp. 844-878.
[29] M. Bellare, D. Bernstein, and S. Tessaro, Hash-function based PRFs: AMAC and its multi-user security, *Advances in Cryptology — Eurocrypt 2016*, LNCS 9665, pp. 566-595.
[30] M. Bellare, A. Boldyreva, and A. O'Neill, Deterministic and efficiently searchable encryption, *Advances in Cryptology — Crypto 2007*, LNCS 4622, pp. 535-552.
[31] M. Bellare, A. Boldyreva, and J. Staddon, Randomness re-use in multi-recipient encryption schemes, *Public Key Cryptography — PKC 2003*, LNCS 2567, pp. 85-99.
[32] M. Bellare, R. Canetti, and H. Krawczyk, Keying hash functions for message authentication, *Advances in Cryptology — Crypto 1996*, LNCS 1109, pp. 1-15.
[33] M. Bellare, R. Canetti, and H. Krawczyk, HMAC: Keyed-hashing for message authentication, Internet RFC 2104, 1997.
[34] M. Bellare, R. Canetti, and H. Krawczyk, A modular approach to the design and analysis of authentication and key exchange protocols, *Proc. 30th Annual ACM Symposium on Theory of Computing — STOC 1998*, pp. 419-428.
[35] M. Bellare and D. Cash, Pseudorandom functions and permutations provably secure against related-key attacks, *Advances in Cryptology — Crypto 2010*, LNCS 6223, pp. 666-684.
[36] M. Bellare, J. Garay, and T. Rabin, Fast batch verification for modular exponentiation and digital signatures, *Advances in Cryptology — Eurocrypt 1998*, LNCS 1403, pp. 236-250.
[37] M. Bellare, J. Garay, and T. Rabin, Fast batch verification for modular exponentiation and digital signatures, available at http://eprint.iacr.org/1998/007.
[38] M. Bellare, O. Goldreich, and A. Mityagin, The power of verification queries in message authentication and authenticated encryption, available at http://eprint.iacr.org/2004/309.
[39] M. Bellare, D. Hofheinz, and E. Kiltz, Subtleties in the definition of IND-CCA: When and how should challenge decryption be disallowed?, *J. Cryptology*, **28** (2015), pp. 29-48.
[40] M. Bellare, C. Nanprempre, and G. Neven, Unrestricted aggregate signatures, *Automata, Languages, and Programming — ICALP 2007*, LNCS 4596, pp. 411-422.
[41] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko, The one-more-RSA inversion problems and the security of Chaum's blind signature scheme, *J. Cryptology*, **16** (2003), pp. 185-215.
[42] M. Bellare and A. Palacio, GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks, *Advances in Cryptology — Crypto 2002*, LNCS 2442, pp. 149-162.
[43] M. Bellare, K. Paterson, and P. Rogaway, Security of symmetric encryption against mass surveillance, *Advances in Cryptology — Crypto 2014*, LNCS 8616, pp. 1-19.
[44] M. Bellare, K. Pietrzak, and P. Rogaway, Improved security analyses for CBC MACs, *Advances in Cryptology — Crypto 2005*, LNCS 3621, pp. 527-545.
[45] M. Bellare and P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, *Proc. First ACM Conference on Computer and Communications Security — CCS '93*, pp. 62-73.
[46] M. Bellare and P. Rogaway, Optimal asymmetric encryption, *Advances in Cryptology — Eurocrypt 1994*, LNCS 950, pp. 92-111.
[47] M. Bellare and P. Rogaway, The security of triple encryption and a framework for code-based game-playing proofs, *Advances in Cryptology — Eurocrypt 2006*, LNCS 4004, pp. 409-426.
[48] C. Berbain, H. Gilbert, and J. Patarin, QUAD: A practical stream cipher with provable security, *Advances in Cryptology — Eurocrypt 2006*, LNCS 4004, pp. 109-128.
[49] C. Berbain, H. Gilbert, and J. Patarin, QUAD: A multivariate stream cipher with provable security, *Journal of Symbolic Computation*, **44** (2009), pp. 1703-1723.
[50] D. Bernhard, G. Fuchsbauer, E. Ghadafi, N. Smart, and B. Warinschi, Anonymous attestation with user-controlled linkability, *International Journal of Information Security*, **12** (2013), pp. 219-249.
[51] D. Bernstein, email to hash-forum@nist.gov, 2 March 2007.
[52] D. Bernstein, Proving tight security for Rabin-Williams signatures, *Advances in Cryptology — Eurocrypt 2008*, LNCS 4965, pp. 70-87.
[53] D. Bernstein, Multi-user Schnorr, revisited, available at http://eprint.iacr.org/2015/996.
[54] D. Bernstein *et al.*, SPHINCS+: Submission to the NIST post-quantum project, 30 November 2017, available at http://sphincs.org/data/sphincs+-specification.pdf.

[55] D. Bernstein and A. Hülsing, Decisional second-preimage resistance: When does SPR imply PRE?, available at http://eprint.iacr.org/2019/492.

[56] D. Bernstein and T. Lange, Never trust a bunny, *Radio Frequency Identification: Security and Privacy Issues — RFIDSec 2012*, LNCS 7739, pp. 137-148.

[57] D. Bernstein and E. Persichetti, Towards KEM unification, available at http://eprint.iacr.org/2018/526.

[58] K. Bhargavan, B. Blanchet, and N. Kobeissi, Verified models and reference implementations for the TLS 1.3 standard candidate, *Proc. 2017 IEEE Symposium on Security and Privacy*, pp. 483-502.

[59] K. Bhargavan, C. Fournet, M. Kohlweiss, A. Pironti, and P. Strub, Implementing TLS with verified cryptographic security, *Proc. 2013 IEEE Symposium on Security and Privacy*, pp. 445-459.

[60] S. Blake-Wilson and A. Menezes, Unknown key-share attacks on the station-to-station (STS) protocol, *Public Key Cryptography — PKC 1999*, LNCS 1560, pp. 156-170.

[61] B. Blanchet and D. Pointcheval, Automated security proofs with sequences of games, *Advances in Cryptology — Crypto 2006*, LNCS 4117, pp. 537-554.

[62] L. Blum, M. Blum, and M. Shub, A simple unpredictable pseudo-random number generator, *SIAM J. Computing*, **15** (1986), pp. 364-383.

[63] J. Bohli, M. Vasco, and R. Steinwandt, Secure group key establishment revisited, *International Journal of Information Security*, **6** (2007), pp. 243-254.

[64] A. Boldyreva, Efficient threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme, *Public Key Cryptography — PKC 2003*, LNCS 2567, pp. 31-46.

[65] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, Order-preserving symmetric encryption, *Advances in Cryptology — Eurocrypt 2009*, LNCS 5479, pp. 224-241.

[66] A. Boldyreva, C. Gentry, A. O'Neill, and D. H. Yum, Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing, *Proc. 14th ACM Conference on Computer and Communications Security — CCS '07*, pp. 276-285; full version available at http://eprint.iacr.org/2007/438.

[67] A. Boldyreva, V. Goyal and V. Kumar, Identity-based encryption with efficient revocation, *Proc. Fifteenth ACM Conference on Computer and Communications Security — CCS '08*, pp. 417-426.

[68] D. Boneh and X. Boyen, Short signatures without random oracles, *Advances in Cryptology — Eurocrypt 2004*, LNCS 3027, pp. 56-73.

[69] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, Public key encryption with keyword search, *Advances in Cryptology — Eurocrypt 2004*, LNCS 3027, pp. 506-522.

[70] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *SIAM J. Computing*, **32** (2003), pp. 586-615.

[71] R. Bost and O. Sanders, Trick or tweak: On the (in)security of OTR's tweaks, *Advances in Cryptology — Asiacrypt 2016*, LNCS 10031, pp. 333-353.

[72] M. Boyarsky, Public-key cryptography and password protocols: The multi-user case, *Proc. 6th ACM Conference on Computer and Communications Security — CCS '99*, pp. 63-72.

[73] C. Boyd and J. Nieto, Round-optimal contributory conference key agreement, *Public Key Cryptography — PKC 2003*, LNCS 2567, pp. 161-174.

[74] C. Boyd and C. Pavlovski, Attacking and repairing batch verification schemes, *Advances in Cryptology — Asiacrypt 2000*, LNCS 1976, pp. 58-71.

[75] E. Bresson, O. Chevassut, and D. Pointcheval, Provably authenticated group Diffie-Hellman key exchange — the dynamic case, *Advances in Cryptology — Asiacrypt 2001*, LNCS 2248, pp. 290-309.

[76] E. Bresson, O. Chevassut, D. Pointcheval, and J. Quisquater, Provably authenticated group Diffie-Hellman key exchange, *Proc. 8th ACM Conference on Computer and Communications Security — CCS '01*, pp. 255-264.

[77] E. Brickell, J. Camenisch, and L. Chen, Direct anonymous attestation, *Proc. 11th ACM Conference on Computer and Communications Security — CCS '04*, pp. 132-145.

[78] E. Brickell, L. Chen, and J. Li, Simplified security notions for direct anonymous attestation and a concrete scheme from pairings, *International Journal of Information Security*, **8** (2009), pp. 315-330.

[79] E. Brickell and J. Li, A pairing-based DAA scheme further reducing TPM resources, *Trust and Trustworthy Computing — Trust 2010*, LNCS 6101, pp. 181-195.

[80] J. Bringer and H. Chabanne, Trusted-HB: A low-cost version of HB^+ secure against man-in-the-middle attacks, *IEEE Transactions on Information Theory*, **54** (2008), pp. 4339-4342.
[81] J. Buchmann, E. Dahmen, S. Ereth, A. Hülsing, and M. Rückert, On the security of the Winternitz one-time signature scheme, *International Journal of Applied Cryptography*, **3** (2013), pp. 84-96.
[82] J. Camenisch, M. Drijvers, and A. Lehmann, Anonymous attestation using the strong Diffie-Hellman assumption revisited, *Trust and Trustworthy Computing — Trust 2016*, LNCS 9824, pp. 1-20.
[83] J. Camenisch, M. Drijvers, and A. Lehmann, Universally composable direct anonymous attestation, *Public Key Cryptography — PKC 2016*, LNCS 9615, pp. 234-264.
[84] J. Camenisch and M. Michels, Confirmer signature schemes secure against adaptive adversaries, *Advances in Cryptology — Eurocrypt 2000*, LNCS 1807, pp. 243-258.
[85] R. Canetti, O. Goldreich, and S. Halevi, The random oracle methodology, revisited, *Journal of the ACM*, **51** (2004), pp. 557-594.
[86] R. Canetti and H. Krawczyk, Analysis of key-exchange protocols and their use for building secure channels, *Advances in Cryptology — Eurocrypt 2001*, LNCS 2045, pp. 453-474.
[87] R. Canetti and H. Krawczyk, Universally composable notions of key exchange and secure channels, *Advances in Cryptology — Eurocrypt 2002*, LNCS 2332, pp. 337-351.
[88] R. Canetti and H. Krawczyk, Security analysis of IKE's signature-based key-exchange protocol, *Advances in Cryptology — Crypto 2002*, LNCS 2442, pp. 143-161.
[89] R. Canetti and T. Rabin, Universal composition with joint state, *Advances in Cryptology — Ceypto 2003*, LNCS 2729, pp. 165-281; extended version 20020419:032235 available at http://eprint.iacr.org/2002/047.
[90] B. Canvel, A. Hiltgen, S. Vaudenay, and M. Vuagnoux, Password interception in a SSL/TLS channel, *Advances in Cryptology — Crypto 2003*, LNCS 2729, pp. 583-599.
[91] D. Chakraborty, V. Hernández-Jiménez, and P. Sarkar, Another look at XCB, *Cryptography and Communications*, **7** (2015), pp. 439-468.
[92] D. Chakraborty and M. Nandi, Attacks on the authenticated encryption mode of operation PAE, *IEEE Transactions on Information Theory*, **61** (2015), pp. 5636-5624.
[93] D. Chakraborty and P. Sarkar, On modes of operations of a block cipher for authentication and authenticated encryption, *Cryptography and Communications*, **8** (2016), pp. 455-511.
[94] H. Chan, A. Perrig, and D. Song, Secure hierarchical in-network aggregation in sensor networks, *Proc. 13th ACM Conference on Computer and Communications Security — CCS '06*, pp. 278-287.
[95] D. Chang, M. Nandi, and M. Yung, On the security of hash functions employing blockcipher post-processing, *Fast Software Encryption — FSE 2011*, LNCS 6733, pp. 146-166.
[96] S. Chatterjee and M. Das, Property preserving symmetric encryption revisited, *Advances in Cryptology — Asiacrypt 2015*, LNCS 9453, pp. 658-682.
[97] S. Chatterjee, C. Kamath, and V. Kumar, Galindo-Garcia identity-based signature revisited, *Information Security and Cryptology — ISC 2012*, LNCS 7839, pp. 456-471.
[98] S. Chatterjee, K. Karabina, and A. Menezes, Fault attacks on pairing-based protocols revisited, *IEEE Transactions on Computers*, **64** (2015), pp. 1707-1714.
[99] S. Chatterjee, N. Koblitz, A. Menezes, and P. Sarkar, Another look at tightness II: Practical issues in cryptography, *Paradigms in Cryptology — Mycrypt 2016*, LNCS 10311, pp. 21-55.
[100] S. Chatterjee, A. Menezes, and P. Sarkar, Another look at tightness, *Selected Areas in Cryptography — SAC 2011*, LNCS 7118, pp. 293-319.
[101] L. Chen, A DAA scheme requiring less TPM resources, *Information Security and Cryptology — Inscrypt 2009*, LNCS 6151, pp. 350-365.
[102] Y. Chen, M. Charlemagne, Z. Guan, J. Hu, and Z. Chen, Identity-based encryption based on DHIES, *Proc. 5th ACM Symposium on Information, Computer and Communications Security — ASIA CCS 2010*, pp. 82-88.
[103] L. Chen, Z. Cheng, and N. Smart, Identity-based key agreement protocols from pairings, *International Journal of Information Security*, **6** (2007), pp. 213-241.
[104] L. Chen and C. Kudla, Identity based authenticated key agreement protocols from pairings, *Proc. 16th IEEE Computer Security Foundations Workshop*, 2003, pp. 219-233.
[105] L. Chen and J. Li, A note on the Chen-Morrissey-Smart DAA scheme, *Information Processing Letters*, **110** (2010), pp. 485-488.

[106] L. Chen and J. Li, Flexible and scalable digital signatures in TPM 2.0, *Proc. 2013 ACM SIGSAC Conference on Computer and Communications Security — CCS '13*, pp. 37-48.
[107] L. Chen, P. Morrissey, and N. Smart, Pairings in trusted computing, *Pairing-Based Cryptography — Pairing 2008*, LNCS 5209, pp. 1-17.
[108] L. Chen, P. Morrissey, and N. Smart, On proofs of security for DAA schemes, *International Conference on Provable Security — ProvSec 2008*, LNCS 5324, pp. 156-175.
[109] L. Chen, D. Page, and N. Smart, On the design and implementation of an efficient DAA scheme, *Smart Card Research and Advanced Applications — CARDIS 2010*, LNCS 6035, pp. 223-237.
[110] J. Cheon, P. Fouque, C. Lee, B. Minaud, and H. Ryu, Cryptanalysis of the new CLT multilinear map over the integers, *Advances in Cryptology — Eurocrypt 2016*, LNCS 9665, pp. 509-536.
[111] J. Cheon, K. Han, C. Lee, H. Ryu, and D. Stehlé, Cryptanalysis of the multilinear map over the integers, *Advances in Cryptology — Eurocrypt 2015*, LNCS 9056, pp. 3-12.
[112] J. Cheon, H. Lee, and J. Seo, A new additive homomorphic encryption based on the co-ACD problem, *Proc. 2014 ACM SIGSAC Conference on Computer and Communications Security — CCS '14*, pp. 287-298.
[113] K. Choo, C. Boyd, and Y. Hitchcock, Errors in computational complexity proofs for protocols, *Advances in Cryptology — Asiacrypt 2005*, LNCS 3788, pp. 624-643.
[114] S. Chow, J. Weng, Y. Yang, and R. Deng, Efficient unidirectional proxy re-encryption, *Progress in Cryptology — Africacrypt 2010*, LNCS 6055, pp. 316-332.
[115] S. Coretti, Y. Dodis, S. Guo, and J. Steinberger, Random oracles and non-uniformity, *Advances in Cryptology — Eurocrypt 2018*, LNCS 10820, pp. 227-258.
[116] J.-S. Coron, On the exact security of full domain hash, *Advances in Cryptology — Crypto 2000*, LNCS 1880, pp. 229-235.
[117] J.-S. Coron, Optimal security proofs for PSS and other signature schemes, *Advances in Cryptology — Eurocrypt 2002*, LNCS 2332, pp. 272-287.
[118] J.-S. Coron, Y. Dodis, C. Malinaud, and P. Puniya, Merkle-Damgård revisited: How to construct a hash function, *Advances in Cryptology — Crypto 2005*, LNCS 3621, pp. 430-448.
[119] J.-S. Coron, H. Handschuh, M. Joye, P. Paillier, D. Pointcheval, and C. Tymen, GEM: A generic chosen-ciphertext secure encryption method, *Topics in Cryptology — CT-RSA 2002*, LNCS 2271, pp. 263-276.
[120] J.-S. Coron, T. Holenstein, R. Künzler, J. Patarin, Y. Seurin, and S. Tessaro, How to build an ideal cipher: The indifferentiability of the Feistel construction, *J. Cryptology*, **29** (2016), pp. 61-114.
[121] J.-S. Coron, A. Joux, A. Mandal, D. Naccache, and M. Tibouchi, Cryptanalysis of the RSA subgroup assumption from TCC 2005, *Public Key Cryptography — PKC 2011*, LNCS 6571, pp. 147-155.
[122] J.-S. Coron, M. Lee, T. Lepoint, and M. Tibouchi, Cryptanalysis of GGH15 multilinear maps, *Advances in Cryptology — Crypto 2016*, LNCS 9815, pp. 607-628.
[123] J.-S. Coron, T. Lepoint, and M. Tibouchi, Practical multilinear maps over the integers, *Advances in Cryptology — Crypto 2013*, LNCS 8042, pp. 476-493.
[124] J.-S. Coron, T. Lepoint, and M. Tibouchi, New multilinear maps over the integers, *Advances in Cryptology — Crypto 2015*, LNCS 9215, pp. 267-286.
[125] J.-S. Coron and D. Naccache, On the security of RSA screening, *Public Key Cryptography — PKC 1999*, LNCS 1560, pp. 197-203.
[126] J.-S. Coron, J. Patarin, and Y. Seurin, The random oracle model and the ideal cipher model are equivalent, *Advances in Cryptology — Crypto 2008*, LNCS 5157, pp. 1-20.
[127] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. van der Merwe, A comprehensive symbolic analysis of TLS 1.3, *Proc. 2017 ACM SIGSAC Conference on Computer and Communications Security — CCS '17*, pp. 1773-1788.
[128] J. Degabriele, P. Farshim, and B. Poettering, A more cautious approach to security against mass surveillance, *Fast Software Encryption — FSE 2015*, LNCS 9054, pp. 579-598.
[129] J. Degabriele, K. Paterson, and G. Watson, Provable security in the real world, *IEEE Security & Privacy*, May/June 2011, pp. 33-41.
[130] R. De Millo, R. Lipton, and A. Perlis, Social processes and proofs of theorems and programs, *Communications of the ACM*, **22** (1979), pp. 271-280.

[131] Y. Dodis, T. Ristenpart, and T. Shrimpton, Salvaging Merkle-Damgård for practical applications, *Advanced in Cryptology — Eurocrypt 2009*, LNCS 5479, pp. 371-388.
[132] D. Dolev, C. Dwork, and M. Naor, Non-malleable cryptography, *SIAM J. Computing*, **30** (2000), pp. 391-437.
[133] M. Drijvers, K. Edalatnejad, B. Ford, E. Kiltz, J. Loss, G. Neven, and I. Stepanovs, On the security of two-round multi-signatures, available at http://eprint.iacr.org/2018/417.
[134] N. Drucker and S. Gueron, Selfie: reflections on TLS 1.3 with PSK, available at http://eprint.iacr.org/2019/347.
[135] T. Duong and J. Rizzo, BEAST: A surprising crypto attack against https, 2012, available at http://antoanthongtin.vn/Portals/0/TempUpload/pProceedings/2014/9/26/tetcon2012_juliano_beast.pdf.
[136] D. Eastlake, S. Crocker, and J. Schiller, *RFC 1750 — Randomness Recommendations for Security*, available at http://www.ietf.org/rfc/rfc1750.txt.
[137] O. Eikemeier *et al.*, History-free aggregate message authentication codes, *Security and Cryptography for Networks — SCN 2010*, LNCS 6280, pp. 309-328.
[138] J. Fan, X. Guo, E. De Mulder, P. Schaumont, B. Preneel, and I. Verbauwhede, State-of-the-art of secure ECC implementations: A survey of known side-channel attacks and countermeasures, *IEEE International Symposium on Hardware-Oriented Security and Trust — HOST 2010*, pp. 76-87.
[139] P. Farshim, B. Libert, K. Paterson, and E. Quaglia, Robust encryption, revisited, *Public Key Cryptography — PKC 2013*, LNCS 7788, pp. 352-368.
[140] S. Fehr, D. Hofheinz, E. Kiltz, and H. Wee, Encryption schemes secure against chosen-ciphertext selective opening attacks, *Advances in Cryptology — Eurocrypt 2010*, LNCS 6110, pp. 381-402.
[141] M. Fischlin and F. Günther, Replay attacks on zero round-trip time: The case of TLS 1.3 handshake candidates, *Proc. 2017 IEEE European Symposium on Security and Privacy*, pp. 60-75.
[142] P. Fouque, M. Lee, T. Lepoint, and M. Tibouchi, Cryptanalysis of the co-ACD assumption, *Advances in Cryptology — Crypto 2015*, LNCS 9215, pp. 561-580.
[143] C. Forler, E. List, S. Lucks, and J. Wenzel, POEx: A beyond-birthday-bound-secure on-line cipher, *ArticCrypt 2016*, available at http://www.researchgate.net/publication/299565944.
[144] D. Freedman, Lies, damned lies, and medical science, *The Atlantic*, **306** (4) (2010), pp. 76-84.
[145] D. Frumkin and A. Shamir, Un-trusted-HB: Security vulnerabilities of trusted-HB, available at http://eprint.iacr.org/2009/044.
[146] G. Fuchsbauer, Breaking existential unforgeability of a signature scheme from Asiacrypt 2014, available at http://eprint.iacr.org/2014/892.
[147] G. Fuchsbauer, C. Hanser, C. Kamath, and D. Slamanig, Practical round-optimal blind signatures in the standard model from weaker assumptions, *Security and Cryptography for Networks — SCN 2016*, LNCS 9841, pp. 391-408.
[148] G. Fuchsbauer, C. Hanser, and D. Slamanig, Practical round-optimal blind signatures in the standard model, *Advances in Cryptology — Crypto 2015*, LNCS 9216, pp. 233-253.
[149] G. Fuchsbauer, C. Hanser, and D. Slamanig, Structure-preserving signatures on equivalence classes and constant-size anonymous credentials, *J. Cryptology*, **32** (2019), pp. 498-546.
[150] J. Furukawa and H. Imai, An efficient group signature scheme from bilinear maps, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E89-A** (2006), pp. 1328-1338.
[151] S. Galbraith, J. Malone-Lee, and N. Smart, Public key signatures in the multi-user setting, *Information Processing Letters*, **83** (2002), pp. 263-266.
[152] D. Galindo, Boneh-Franklin identity-based encryption revisited, *Automata, Languages and Programming — ICALP 2005*, LNCS 3580, pp. 791-802.
[153] D. Galindo and F. García, A Schnorr-like lightweight identity-based signature scheme, *Progress in Cryptology — Africacrypt 2009*, LNCS 5580, pp. 135-148.
[154] S. Garg, C. Gentry, and S. Halevi, Candidate multilinear maps from ideal lattices, *Advances in Cryptology — Eurocrypt 2013*, LNCS 7881, pp. 1-17.
[155] S. Garg and D. Gupta, Efficient round optimal blind signatures, *Advances in Cryptology — Eurocrypt 2014*, LNCS 8441, pp. 477-495.
[156] P. Gaži and U. Maurer, Cascade encryption revisited, *Advances in Cryptology — Asiacrypt 2009*, LNCS 5912, pp. 37-51.

[157] R. Gennaro, S. Halevi, and T. Rabin, Secure hash-and-sign signatures without the random oracle, *Advances in Cryptology —- Eurocrypt 1999*, LNCS 1592, pp. 123-139.

[158] C. Gentry, S. Gorbunov, and S. Halevi, Graph-induced multilinear maps from lattices, *Theory of Cryptography Conference — TCC 2015*, LNCS 9015, pp. 498-527.

[159] C. Gentry, D. Molnar, and Z. Ramzan, Efficient designated confirmer signatures without random oracles or general zero-knowledge proofs, *Advances in Cryptology — Asiacrypt 2005*, LNCS 3788, pp. 662-681.

[160] F. Giacon, E. Kiltz, and B. Poettering, Hybrid encryption in a multi-user setting, revisited, *Public Key Cryptography — PKC 2018*, LNCS 10769, pp. 159-189.

[161] H. Gilbert, M. Robshaw, and H. Sibert, Active attack against HB^+: A provably secure lightweight authentication protocol, *Electronics Letters*, **41** (2005), pp. 1169-1170.

[162] O. Goldreich, On post-modern cryptography, available at http://eprint.iacr.org/2006/461.

[163] S. Goldwasser and M. Bellare, Lecture Notes on Cryptography, July 2008, available at http://cseweb.ucsd.edu/mihir/papers/gb.pdf.

[164] S. Goldwasser and Y. Kalai, Cryptographic assumptions: A position paper, available at http://eprint.iacr.org/2015/907.

[165] S. Goldwasser, S. Micali, and R. Rivest, A "paradoxical" solution to the signature problem, *Proc. 25th Annual IEEE Symposium on the Foundations of Computer Science — FOCS 1984*, pp. 441-448.

[166] S. Goldwasser and E. Waisbard, Transformation of digital signature schemes into designated confirmer signature schemes, *Theory of Cryptography Conference — TCC 2004*, LNCS 2951, pp. 77-100.

[167] B. Gong and Y. Zhao, Cryptanalysis of RLWE-based one-pass authenticated key exchange, *Post-Quantum Cryptography — PQCrypto 2017*, LNCS 10346, pp. 163-183.

[168] R. Granger, On the static Diffie-Hellman problem on elliptic curves over extension fields, *Advances in Cryptology — Asiacrypt 2010*, LNCS 6477, pp. 283-302.

[169] J. Groth, Cryptography in subgroups of Z_n^*, *Theory of Cryptography Conference — TCC 2005*, LNCS 3378, pp. 50-65.

[170] P. Grubbs, R. McPherson, M. Naveed, T. Ristenpart, and V. Shmatikov, Breaking web applications built on top of encrypted data, *Proc. 2016 ACM SIGSAC Conference on Computer and Communications Security —CCS '16*, pp. 1353-1364.

[171] P. Grubbs, T. Ristenpart, and V. Shmatikov, Why your encrypted database is not secure, *Proc. 16th Workshop on Hot Topics in Operating Systems — HotOS 2017*, ACM, pp. 162-168.

[172] S. Halevi, An observation regarding Jutla's modes of operation, available at http://eprint.iacr.org/2001/015.

[173] S. Halevi, A plausible approach to computer-aided cryptographic proofs, available at http://eprint.iacr.org/2005/181.

[174] S. Halevi and H. Krawczyk, Public-key cryptography and password protocols, *Proc. 5th ACM Conference on Computer and Communications Security — CCS '98*, pp. 122-131.

[175] S. Halevi and P. Rogaway, A parallelizable enciphering mode, *Topics in Cryptology — CT-RSA 2004*, LNCS 2964, pp. 292-304.

[176] C. Hanser and D. Slamanig, Structure-preserving signatures on equivalence classes and their application to anonymous credentials, *Advances in Cryptology — Asiacrypt 2014*, LNCS 8873, pp. 491-511.

[177] C. Herley and P. van Oorschot, SoK: Science, security and the elusive goal of security as a scientific pursuit, *Proc. 2017 IEEE Symposium on Security and Privacy*, pp. 99-120.

[178] G. Herold, Polly cracker, revisited, revisited, *Public Key Cryptography — PKC 2012*, LNCS 7293, pp. 17-33.

[179] S. Heyse, E. Kiltz, V. Lyubashevsky, C. Paar, and K. Pietrzak, Lapin: An efficient authentication protocol based on ring-LPN, *Fast Software Encryption — FSE 2012*, LNCS 7549, pp. 346-365.

[180] D. Hofheinz, K. Hövelmanns, and E. Kiltz, A modular analysis of the Fujisaki-Okamoto transformation, *Theory of Cryptography Conference — TCC 2017*, LNCS 10677, pp. 341-371.

[181] D. Hofheinz, K. Hövelmanns, and E. Kiltz, A modular analysis of the Fujisaki-Okamoto transformation, available at http://eprint.iacr.org/2017/604.

[182] T. Holenstein, R. Künzler, and S. Tessaro, The equivalence of the random oracle model and the ideal cipher model, revisited, *Proc. 43rd Annual ACM Symposium on Theory of Computing — STOC 2011*, pp. 89-98.

[183] Y. Hu and H. Jia, Cryptanalysis of GGH map, *Advances in Cryptology — Eurocrypt 2016*, LNCS 9665, pp. 537-565.
[184] Y. Huang, F. Liu, and B. Yang, Public-key cryptography from new multivariate quadratic assumptions, *Public Key Cryptography — PKC 2012*, LNCS 7293, pp. 190-205.
[185] Z. Huang, S. Liu, and B. Qin, Sender-equivocable encryption schemes secure against chosen-ciphertext attacks revisited, *Public Key Cryptography — PKC 2013*, LNCS 7778, pp. 369-385.
[186] D. Huff, *How to Lie with Statistics*, W. W. Norton, 1954.
[187] E. Hufschmitt and J. Traoré, Fair blind signatures revisited, *Pairing-Based Cryptography — Pairing 2007*, LNCS 4575, pp. 268-292.
[188] A. Hülsing, J. Rijnveld, and F. Song, Mitigating multi-target attacks in hash-based signatures, *Public Key Cryptography — PKC 2016*, LNCS 9614, pp. 387-417.
[189] J. Hwang, D. Lee, and M. Yung, Universal forgery of the identity-based sequential aggregate signature scheme, *Proc. 4th International Symposium on Information, Computer and Communications Security — ASIA CCS 2009*, ACM, pp. 157-160.
[190] Y. Hwang and P. Lee, Public key encryption with conjunctive keyword search and its extension to a multi-user system, *Pairing-Based Cryptography — Pairing 2007*, LNCS 4575, pp. 2-22.
[191] A. Inoue, T. Iwata, K. Minematsu, and B. Poettering, Cryptanalysis of OCB2: Attacks on authenticity and confidentiality, available at http://eprint.iacr.org/2019/311.
[192] A. Ishida, Y. Sakai, K. Emura, G. Hanaoka, and K. Tanaka, Proper usage of the group signature scheme in ISO/IEC 20008-2, available at http://eprint.iacr.org/2019/284.
[193] ISO/IEC 19772:2009, Information Technology — Security Techniques — Authenticated Encryption, 2009.
[194] T. Iwata, K. Ohashi, and K. Minematsu, Breaking and repairing GCM security proofs, *Advances in Cryptology — Crypto 2012*, LNCS 7417, pp. 31-49.
[195] M. Jakobsson and D. Pointcheval, Mutual authentication for low-power mobile devices, *Financial Cryptography — FC 2001*, LNCS 2339, pp. 178-195.
[196] A. Jha and M. Nandi, Revisiting structure graphs: Applications to CBC-MAC and EMAC, *J. Math. Cryptology*, **10** (2016), pp. 157-180.
[197] A. Jha and M. Nandi, On rate-1 and beyond-the-birthday bound secure online ciphers using tweakable block ciphers, *Cryptography and Communications*, **10** (2018), pp 731-753.
[198] A. Joux, G. Martinet, and F. Valette, Block-adaptive attackers: Revisiting the (in)security of some provably secure encryption modes: CBC, GEM, 1ACBC, *Advances in Cryptology — Crypto 2002*, LNCS 2442, pp. 17-30.
[199] A. Juels and S. Weis, Authenticating pervasive devices with human protocols, *Advances in Cryptology — Crypto 2005*, LNCS 3621, pp. 293-308.
[200] S. Kakvi and E. Kiltz, Optimal security proofs for full domain hash, revisited, *Advances in Cryptology — Eurocrypt 2012*, LNCS 7237, pp. 537-553.
[201] J. Katz, Letter to the editor, *Notices of the Amer. Math. Soc.*, **54** (2007), pp. 1454-1455.
[202] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd edition, Chapman and Hall/CRC, 2014.
[203] J. Katz and Y. Lindell, Aggregate message authentication codes, *Topics in Cryptology — CT-RSA 2008*, LNCS 4964, pp. 155-169.
[204] E. Kiltz, D. Masny, and J. Pan, Optimal security proofs for signatures from identification schemes, *Advances in Cryptology — Crypto 2016*, LNCS 9815, pp. 33-61.
[205] A. H. Koblitz, N. Koblitz, and A. Menezes, Elliptic curve cryptography: The serpentine course of a paradigm shift, *J. Number Theory*, **131** (2011), pp. 781-814.
[206] N. Koblitz, The uneasy relationship between mathematics and cryptography, *Notices of the Amer. Math. Soc.*, **54** (2007), pp. 972-979.
[207] N. Koblitz, Another look at automated theorem-proving, *J. Math. Cryptology*, **1** (2007), pp. 385-403.
[208] N. Koblitz, Another look at automated theorem-proving. II, *J. Math. Cryptology*, **5** (2011), pp. 205-224.
[209] N. Koblitz and A. Menezes, Another look at provable security. II, *Progress in Cryptology — Indocrypt 2006*, LNCS 4329, pp. 148-175.
[210] N. Koblitz and A. Menezes, Another look at provable security, *J. Cryptology*, **20** (2007), pp. 3-37.

[211] N. Koblitz and A. Menezes, Another look at generic groups, *Advances in Math. Communications*, **1** (2007), pp. 13-28.
[212] N. Koblitz and A. Menezes, Another look at non-standard discrete log and Diffie-Hellman problems, *J. Math. Cryptology*, **2** (2008), pp. 311-326.
[213] N. Koblitz and A. Menezes, The brave new world of bodacious assumptions in cryptography, *Notices of the Amer. Math. Soc.*, **57** (2010), pp. 357-365.
[214] N. Koblitz and A. Menezes, Intractible problems in cryptography, http://eprint.iacr.org/2010/290 and *Finite Fields: Theory and Applications, Contemporary Mathematics*, **518** (2010), pp. 279-300.
[215] N. Koblitz and A. Menezes, Another look at HMAC, *J. Math. Cryptology*, **7** (2013), pp. 225-251.
[216] N. Koblitz and A. Menezes, Another look at non-uniformity, *Groups Complexity Cryptology*, **5** (2013), pp. 117-139.
[217] N. Koblitz and A. Menezes, Another look at security definitions, *Advances in Math. Communications*, **7** (2013), pp. 1-38.
[218] N. Koblitz and A. Menezes, Another look at security theorems for 1-key nested MACs, in Ç. Koç, ed., *Open Problems in Mathematics and Computational Science*, Springer-Verlag, 2014, pp. 69-89.
[219] N. Koblitz and A. Menezes, The random oracle model: A twenty-year retrospective, *Designs, Codes and Cryptography*, **77** (2015), pp. 587-610.
[220] H. Krawczyk, The order of encryption and authentication for protecting communications (or: How secure is SSL?), *Advances in Cryptology — Crypto 2001*, LNCS 2139, pp. 310-331.
[221] H. Krawczyk, HMQV: A high-performance secure Diffie-Hellman protocol, *Advances in Cryptology — Crypto 2005*, LNCS 3621, pp. 546-566.
[222] S. Kunz-Jacques, G. Martinet, G. Poupard, and J. Stern, Cryptanalysis of an efficient proof of knowledge of discrete logarithm, *Public Key Cryptography — PKC 2006*, LNCS 3958, pp. 27-43.
[223] K. Kurosawa and W. Ogata, Efficient Rabin-type digital signature scheme, *Designs, Codes and Cryptography*, **16** (1999), pp. 53-64.
[224] M. Lacharité, Security of BLS and BGLS signatures in a multi-user setting, *Cryptography and Communications*, **10** (2018), pp. 41-58.
[225] P. Lafrance and A. Menezes, On the security of the WOTS-PRF signature scheme, *Advances in Math. Communications*, **13** (2019), pp. 185-193.
[226] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, An efficient protocol for authenticated key agreement, *Designs, Codes and Cryptography*, **28** (2003), pp. 119-134.
[227] G. Leurent, M. Nandi, and F. Sibleyras, Generic attacks against beyond-birthday-bound MACs, *Advances in Cryptology — Crypto 2018*, LNCS 10992, pp. 306-336.
[228] B. Libert and J. Quisquater, Efficient signcryption with key privacy from gap Diffie-Hellman groups, *Public Key Cryptography — PKC 2004*, LNCS 2947, pp. 187-200.
[229] B. Libert and J. Quisquater, Improved signcryption from q-Diffie-Hellman problems, *Security in Communication Networks — SCN 2004*, LNCS 3352, pp. 220-234.
[230] E. List and M. Nandi, Revisiting full-prf-secure PMAC and using it for beyond-birthday authenticated encryption, *Topics in Cryptology — CT-RSA 2017*, LNCS 10159, pp. 258-274.
[231] A. Luykx, B. Mennink, and K. Paterson, Analyzing multi-key security degradation, *Advances in Cryptology — Asiacrypt 2017*, LNCS 10625, pp. 575-605.
[232] C. Ma, Efficient short signcryption scheme with public verifiability, *Information Security and Cryptology — Inscrypt 2006*, LNCS 4318, pp. 118-129.
[233] C. Ma, J. Weng, Y. Li, and R. Deng, Efficient discrete logarithm based multi-signature scheme in the plain public key model, *Designs, Codes and Cryptography*, **54** (2010), pp. 121-133.
[234] J. Manger, A chosen ciphertext attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as standardized in PKCS #1 v2.0, *Advances in Cryptology — Crypto 2001*, LNCS 2139, pp. 230-238.
[235] D. McGrew and S. Fluhrer, The security of the extended codebook (XCB) mode of operation, *Selected Areas in Cryptography — SAC 2007*, LNCS 4876, pp. 311-327.
[236] D. McGrew and J. Viega, The security and performance of the Galois/Counter Mode (GCM) of operation, *Progress in Cryptology — Indocrypt 2004*, LNCS 3348, pp. 343-355.
[237] A. Menezes, Another look at HMQV, *J. Math. Cryptology*, **1** (2007), pp. 47-64.
[238] A. Menezes, Another look at provable security, Invited talk at Eurocrypt 2012, available at http://www.cs.bris.ac.uk/eurocrypt2012/Program/Weds/Menezes.pdf.

[239] A. Menezes and N. Smart, Security of signature schemes in a multi-user setting, *Designs, Codes and Cryptography*, **33** (2004), pp. 261-274.
[240] A. Menezes and B. Ustaoglu, On the importance of public-key validation in the MQV and HMQV key agreement protocols, *Progress in Cryptology — Indocrypt 2006*, LNCS 4329, pp. 133-147.
[241] K. Minematsu, Parallelizable rate-1 authenticated encryption from pseudorandom functions, *Advances in Cryptology — Eurocrypt 2014*, LNCS 8441, pp. 275-292.
[242] B. Möller, T. Duong, and K. Kotowicz, The POODLE bites: Exploiting the SSL 3.0 fallback, 2014, available at http://www.openssl.org/~bodo/ssl-poodle.pdf.
[243] Y. Naito, Full prf-secure message authentication code based on tweakable block cipher, *International Conference on Provable Security — ProvSec 2015*, LNCS 9451, pp. 167-182.
[244] Y. Naito, Improved security bound of LightMAC_Plus and its single-key variant, *Topics in Cryptology — CT-RSA 2018*, LNCS 10808, pp. 300-318.
[245] M. Nandi, Forging attacks on two authenticated encryption schemes COBRA and POET, *Advances in Cryptology — Asiacrypt 2014*, LNCS 8873, pp. 126-140.
[246] M. Nandi, XLS is not a strong pseudorandom permutation, *Advances in Cryptology — Asiacrypt 2014*, LNCS 8873, pp. 478-490.
[247] M. Nandi and T. Pandit, On the security of joint signature and encryption revisited, *J. Math. Cryptology*, **10** (2016), pp. 181-221.
[248] T. Okamoto, E. Fujisaki, and H. Morita, TSH-ESIGN: Efficient digital signature scheme using trisection hash, submission to IEEE P1363a, 1998.
[249] C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown, 2016.
[250] O. Pandey and Y. Rouselakis, Property preserving symmetric encryption, *Advances in Cryptology — Eurocrypt 2012*, LNCS 7237, pp. 375-391.
[251] D. Park, K. Kim, and P. Lee, Public-key encryption with conjunctive keyword search, *WISA 2004*, LNCS 3325, pp. 73-86.
[252] K. Paterson, T. Ristenpart, and T. Shrimpton, Tag size *does* matter: Attacks and proofs for the TLS record protocol, *Advances in Cryptology — Asiacrypt 2011*, LNCS 7073, pp. 372-389.
[253] C. Peikert, 19 February 2015 blog posting, http://web.eecs.umich.edu/~cpeikert/soliloquy.html.
[254] C. Peikert, 24 May 2018 pqc-forum, http://groups.google.com/a/list.nist.gov/forum/#!topic/pqc-forum/7H6wv-Xrp18.
[255] K. Pietrzak, A tight bound for EMAC, *Automata, Languages and Programming. Part II — ICALP 2006*, LNCS 4052, pp. 168-179.
[256] A. Pinto, B. Poettering, and J. Schuldt, Multi-recipient encryption, revisited, *Proc. 9th ACM Symposium on Information, Computer and Communications Security — ASIA CCS '14*, pp. 229-238.
[257] R. Poddar, T. Boelter, and R. Popa, Arx: A strongly encrypted database system, available at http://eprint.iacr.org/2016/591.
[258] D. Pointcheval and J. Stern, Security arguments for digital signatures and blind signatures, *J. Cryptology*, **13** (2000), pp. 361-396.
[259] R. Popa and N. Zeldovich, Multi-key searchable encryption, available at http://eprint.iacr.org/2013/508.
[260] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, *Journal of the ACM*, **56** (6) (2009), p. 34.
[261] T. Ristenpart and P. Rogaway, How to enrich the message space of a cipher, *Fast Software Encryption — FSE 2007*, LNCS 4593, pp. 101-118.
[262] P. Rogaway, Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC, *Advances in Cryptology — Asiacrypt 2004*, LNCS 3329, pp. 16-31.
[263] P. Rogaway, M. Bellare, and J. Black, OCB: A block-cipher mode of operation for efficient authenticated encryption, *ACM Transactions on Information and System Security*, **6** (2003), pp. 365-403.
[264] P. Rogaway and T. Shrimpton, A provable-security treatment of the key-wrap problem, *Advances in Cryptology — Eurocrypt 2006*, LNCS 4004, pp. 373-390.
[265] F. Salmon, Recipe for disaster: The formula that killed Wall Street, *Wired Magazine*, **17** (3) (2009).
[266] P. Sarkar, Pseudo-random functions and parallelizable modes of operations of a block cipher, *IEEE Transactions on Information Theory*, **56** (2010), pp. 4025-4037.

[267] C.-P. Schnorr, Efficient identification and signatures for smart cards, *Advances in Cryptology — Crypto 1989*, LNCS 435, pp. 239-252.
[268] C. Schnorr and M. Jakobsson, Security of signed ElGamal encryption, *Advances in Cryptology — Asiacrypt 2000*, LNCS 1976, pp. 73-89.
[269] D. Schröder and D. Unruh, Security of blind signatures revisited, *J. Cryptology*, **30** (2017), pp. 470-494.
[270] W. Schroé, B. Mennink, E. Andreeva, and B. Preneel, Forgery and subkey recovery on CAESAR candidate iFeed, *Selected Areas in Cryptography — SAC 2015*, LNCS 9566, pp. 197-204.
[271] J. Seo and K. Emura, Revocable identity-based encryption revisited: Security model and construction, *Public Key Cryptography — PKC 2013*, LNCS 7778, pp. 216-234.
[272] J. Shao and Z. Cao, CCA-secure proxy re-encryption without pairings, *Public Key Cryptography — PKC 2009*, LNCS 5443, pp. 357-376.
[273] V. Shoup, Lower bounds for discrete logarithms and related problems, *Advances in Cryptology — Eurocrypt 1997*, LNCS 1233, pp. 256-266.
[274] V. Shoup, Why chosen ciphertext security matters, IBM Research Report RZ 3076 (#93122), 23 November 1998.
[275] V. Shoup, OAEP reconsidered, *J. Cryptology*, **15** (2002), pp. 223-249.
[276] V. Shoup, ISO/IEC 18033-2:2006, *Information Technology — Security Techniques — Encryption Algorithms — Part 2: Asymmetric Ciphers*, 2006; final draft available at http://www.shoup.net/iso/std6.pdf.
[277] A. Sidorenko and B. Schoenmakers, Concrete security of the Blum-Blum-Shub pseudorandom generator, *Cryptography and Coding 2005*, LNCS 3796, pp. 355-375.
[278] B. Snow, Telephone conversation with N. Koblitz, 7 May 2009.
[279] A. Sokal, Transgressing the boundaries: Toward a transformative hermeneutics of quantum gravity, *Social Text*, 1996, pp. 217-252.
[280] D. Soldera, J. Seberry, and C. Qu, The analysis of Zheng-Seberry scheme, *ACISP 2002*, LNCS 2384, pp. 159-168.
[281] P. Soundararajan, Non-Constructivity in Security Proofs, Master's thesis, University of Waterloo, 2018.
[282] J. Stern, D. Pointcheval, J. Malone-Lee, and N. Smart, Flaws in applying proof methodologies to signature schemes, *Advances in Cryptology — Crypto 2002*, LNCS 2442, pp. 93-110.
[283] J. Stillwell, *Mathematics and Its History*, 2nd ed., Springer-Verlag, 2002.
[284] C. Tan, On the security of signcryption scheme with key privacy, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E88-A** (2005), pp. 1093-1095.
[285] C. Tan, Analysis of improved signcryption scheme with key privacy, *Information Processing Letters*, **99** (2006), pp. 135-138.
[286] C. Tan, Security analysis of signcryption scheme from q-Diffie-Hellman problems, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E89-A** (2006), pp. 206-208.
[287] C. Tan, Forgery of provable secure short signcryption scheme, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E90-A** (2007), pp. 1879-1880.
[288] M. Tibouchi, Cryptographic multilinear maps: A status report, CRYPTREC-EX-2603-2016, January 2017, available at http://www.cryptrec.go.jp/estimation/cryptrec-ex-2603-2016.pdf.
[289] S. Vaudenay, Security flaws induced by CBC padding — applications to SSL, IPSEC, WTLS, *Advances in Cryptology — Eurocrypt 2002*, LNCS 2332, pp. 534-545.
[290] U. V. Vazirani and V. V. Vazirani, Efficient and secure pseudo-random number generation, *Proc. 25th Annual IEEE Symposium on the Foundations of Computer Science — FOCS 1984*, pp. 458-463.
[291] D. Wikström, Designated confirmer signatures revisited, *Theory of Cryptography Conference — TCC 2007*, LNCS 4392, pp. 342-361.
[292] D. Wong and A. Chan, Efficient and mutually authenticated key exchange for low power computing devices, *Advances in Cryptology — Asiacrypt 2001*, LNCS 2248, pp. 272-28.
[293] Xbox 360 timing attack, http://beta.ivc.no/wiki/index.php/Xbox_360_Timing_Attack.
[294] L. Xi, K. Yang, Z. Zhang, and D. Feng, DAA-related APIs in TPM 2.0 revisited, *Trust and Trustworthy Computing — Trust 2014*, LNCS 8564, pp. 1-18.

[295] B. Yang, C. Chen, D. Bernstein, and J. Chen, Analysis of QUAD, *Fast Software Encryption — FSE 2007*, LNCS 4593, pp. 290-308.
[296] G. Yang, D. Wong, and X. Deng, Analysis and improvement of a signcryption scheme with key privacy, *Information Security — ISC 2005*, LNCS 3650, pp. 218-232.
[297] A. Young and M. Yung, *Malicious Cryptography: Exposing Cryptovirology*, Wiley, 2004.
[298] G. M. Zaverucha, Hybrid encryption in the multi-user setting, available at http://eprint.iacr.org/2012/159.
[299] L. Zhang, W. Hu, H. Sui, and P. Wang, iFeed[AES] v1, submission to CAESAR competition. Available at https://competitions.cr.yp.to/round1/ifeedaesv1.pdf.
[300] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö. Dagdelen, Authenticated key exchange from ideal lattices, *Advances in Cryptology — Eurocrypt 2015*, LNCS 9057, pp. 719-751.

Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195 U.S.A.

E-mail address: koblitz@uw.edu

Department of Combinatorics & Optimization, University of Waterloo, Waterloo, Ontario N2L 3G1 Canada

E-mail address: ajmeneze@uwaterloo.ca