Time for a Paradigm Shift in Our Disciplinary Culture?

Neal Koblitz

Department of Mathematics, University of Washington
koblitz@uw.edu

1 Introduction

The well-known KISS principle of engineering — *Keep It Simple, Stupid!* — is also of value in cryptography. In certain subfields, such as lattice-based crypto and indistinguishability obfuscation, the proposed constructions pay little heed to the KISS principle. Even the descriptions of the proper functioning of the protocols are frightfully complicated (by comparison with RSA or ECC, for example), and the security analyses and guidelines for parameter selection are even more problematic.

But even something as wonderful as the KISS principle can be taken too far, as I learned to my chagrin during my early years of work in cryptography. In the late 1980s, when I wrote or spoke about ECC, I wanted to use the simplest possible examples, and these were the supersingular curves. For instance, just take the equation $y^2 = x^3 - x$ over a field of p elements with $p \equiv 3 \pmod 4$ or else $y^2 = x^3 - 1$ with $p \equiv 2 \pmod 3$, where p is chosen so that respectively $(p+1)/4$ or $(p+1)/6$ is prime. As long as $\log_2 p \geq 163$ we would have 80 bits of security, which at the time was enough.

A few years later, Menezes–Okamoto–Vanstone [14] showed that the discrete log problem (DLP) on such a curve can be reduced to the DLP in the finite field of p^2 elements, and even in the early 1990s this was insecure.

A short time later, when I proposed Hyperelliptic Curve Cryptography (HCC), I again made a very erroneous judgment about parameter selection. My favorite example was a genus-191 hyperelliptic curve over the field of 2 elements whose jacobian has group order divisible by a prime of more than 160 bits. So I was confident in its security. In fact, I thought that a high-genus curve would be more secure than a low-genus one. I couldn't have been more wrong! Although the genus is a measure of the topological complexity of the curve, it was a rookie mistake for me to confuse that with the computational complexity of the corresponding DLP. In 1994, Adleman–DeMarrais–Huang [1] found a subexponential-time algorithm for the DLP on high-genus curves. As a result, my genus-191 example was totally insecure, even in 1994. At present, based on work of Gaudry, Diem, and others, we believe that HCC with $g \geq 3$ is less secure than ECC (which is the $g = 1$ case of HCC); the case $g = 2$ is the only one that seems to be as secure as ECC.

In this way I learned early on how easy it is to make serious mistakes in cryptography. Making mistakes is not necessarily a bad thing if we learn from

them, and one lesson to be learned is to exercise caution in giving assurances to each other and to the general public. We should present our results with care and humility. The pressures on us — characteristic of a modern capitalist, consumer society — to act like salespeople, advertisers, and hypesters, should be resisted.

One expects to encounter giant egos among entrepreneurs, professional athletes, media celebrities, and (especially in the U.S.) politicians. In contrast, a long historical tradition in the intellectual professions, including science and mathematics, has been to discourage

- extreme competitiveness;
- boastfulness and self-promotion;
- aggressive marketing of one's own work;
- angry, intemperate responses to criticism;
- arrogance.

However, the disciplinary culture of our community has become remarkably tolerant of aberrant behavior by researchers — and the worst conduct is sometimes by very prominent people. We have strayed far from the standards that one would expect from scientists. With alarming frequency we see

- abstracts and introductions to papers that exaggerate the authors' contributions with misleading and inaccurate claims;
- shameless self-promotion in invited talks;
- arrogance toward those who belong to different subdisciplines or social groups;
- anger and retaliation in response to criticism, or simply ignoring work that questions the prevailing notions.

2 Important Work Gets Dismissed or Ignored

I will give two examples. First, in the late 1990s, Blake-Wilson and Menezes [4] showed that certain standardized signature protocols (but not all) are vulnerable to an attack that they named the Duplicate Signature Key Selection (DSKS) attack. To illustrate how such an attack works, let's take the example of an online lottery. Alice chooses her number N and sends it in with her signature $s_{\text{Alice}}(N)$. If her number wins, she claims her winnings by showing her certified public key to the officials, who verify that the signature on the winning number was hers.

But before Alice gets around to doing this, a thief named Bob computes a key pair that satisfies the condition that the same signature on N verifies as his, that is, $s_{\text{Bob}}(N) = s_{\text{Alice}}(N)$. He quickly gets it certified and claims the money before Alice shows up.

DSKS attacks have never attracted the interest of people working in provable security. They've been mentioned briefly by Canetti and Dodis, but only in order to dismiss them as unimportant. It is true that DSKS does not violate security of signature schemes under the standard Goldwasser–Micali–Rivest (GMR) security model [6]. But the GMR definition was formulated in 1984, way before anyone was thinking of online lotteries as an application of a signature scheme.

It seems a little imprudent to rigidly adhere to a 1/3-century old definition even after it has been shown to be inadequate in certain settings. For more details, see [10].

A second example of work that deserves to be much better known than it is concerns hybrid encryption schemes. Five years ago Greg Zaverucha posted an important analysis [16] of the security of such schemes in the multi-user setting, which, obviously, is where they are normally deployed. He found practical attacks on certain implementations that had been developed by H. Krawczyk and others and had been "proved secure" by them — but of course only in the single-user setting. Zaverucha's work has been all but ignored by provable security researchers. For more details see [16] and Appendix B to the article [5] in this volume.

3 Exaggerated Advertising of One's Own Work

I'll give two examples, both from leading members of our profession. First, here's an excerpt from the introduction to a widely-cited Micali–Reyzin paper [15] on leakage resilience:

> We focus on the strongest possible adversary, so as to capture what is cryptographically possible in the worst possible, physically observable setting. In particular, we
> • consider an adversary that has full (and indeed adaptive) access to any leaked information; ...
> • construct pseudorandom generators that are provably secure against all physical-observation attacks.
> Our model makes it easy to meaningfully restrict the power of our general physically observing adversary.

Reading these paragraphs could give the practical cryptographer false hopes. Despite the extravagant promises, the paper contains no concrete construction of any pseudorandom generator, let alone one that resists side-channel attacks. Nor do the authors give any techniques that "make it easy to meaningfully restrict the power" of the side-channel attacker.

A second example is from Hugo Krawczyk's invited talk at Asiacrypt 2010. In it Krawczyk described how his work (along with Bellare and Canetti) in developing HMAC in the 1990s had to satisfy both the engineers and theoreticians and achieve a balance between practicality and theoretical soundness. His slide concluded: "Balance regained, and the rest is history."

This was the first time I saw the expression "the rest is history" used about the speaker's own work! Normally one uses that expression about what someone else did. For instance, one can say, "In the 17th century Leibniz and Newton invented calculus, and the rest is history." Or, "In 1939 Einstein signed a letter to U.S. President Roosevelt urging him to start a nuclear weapons program, and the rest is history."

In the mathematical world, I could not imagine someone saying, "In the 1990s I did such-and-such, and the rest is history." That level of boastfulness would be considered socially unacceptable among mathematicians and, I believe, scientists in most fields. But in our community no one bats an eyelash.

And HMAC is not beyond controversy, although the words "the rest is history" would imply that it is.

In 2012 Menezes and I showed that the main concrete security guarantee for the pseudorandom-function property of HMAC that was claimed by Bellare [2] at Crypto 2006 was based on flawed reasoning. It now seems that no practically meaningful prf-property of the sort in Bellare's paper can be proved for HMAC if it is implemented with MD5 or SHA-1.

In addition, in a recent paper on 1-key nested MACs [11] Menezes and I showed that the same security theorems (the tight reduction for the secure-MAC property and the nontight reduction for the prf-property) can be proved for a broad class of MACs, and there's no good reason to believe that the HMAC construction is the best in this class for either security or efficiency.

4 Responses to Criticism

One way to distinguish a healthy disciplinary culture from an unhealthy one is to examine the way leaders of the field respond to criticism. How did Bellare react to our critique of his Crypto 2006 paper, which we posted in February 2012? He wrote me [3]:

> I find your current manuscript insulting to me personally and also wrongful in the way it represents the field. I had in the past been supportive of the goals of the Another Look series, [unlike] most cryptographers I know, who have reacted violently to every paper in the series...

This is amazing — "reacted violently to every paper in the series"! Is this a rational response?

Bellare has never responded publicly to the specific criticism of the fallacy in his concrete security analysis for HMAC. Rather, he has simply accused Menezes and me of being ignorant of the basics of modern cryptography. His failure to deal seriously with this issue is especially regrettable because the security of HMAC is not just a theoretical question — HMAC is one of the most popular and widely-used message authentication codes.

My second example concerns a prominent researcher's reaction to criticism of a flaw in his Crypto 2005 paper [12]. In that paper Krawczyk described his modified version of the Menezes–Qu–Vanstone key agreement protocols, which he called HMQV. He claimed that by supplying a proof of security that did not require a certain step of the original MQV protocol, he could increase efficiency at the same time as he proved security. Astoundingly, the Crypto program committee had accepted the paper after a superficial reading without asking any of the designers of MQV for comment.

The omitted MQV step was a public key validation that had been introduced to prevent known attacks. When Menezes finally got to see the paper, he immediately saw that some of Krawczyk's protocols fell victim to the same attacks. How could this be, if they're "provably secure" without the public key validation?

Menezes started reading the proof carefully, and soon found a glaring flaw (see [13] for details). Krawczyk — and the Program Committee — had been so mesmerized by the (fallacious) proof that they had failed to see the vulnerability.

How did Krawczyk react to this embarrassing setback to HMQV? He denied that it was of any importance, and responded angrily when I described this episode in a 2007 article [8] in the *Notices of the Amer. Math. Society*. In a letter to the *Notices* he wrote:

> Contrary to what Koblitz claims, the HMQV work represents a prime example of the success of theoretical cryptography, not only in laying rigorous mathematical foundations for cryptography at large, but also in its ability to guide us in the design of truly practical solutions to real-world problems.

Part of what provable security researchers mean by the last phrase (as explained, for example, in [7]) is that they can improve efficiency by dropping unnecessary steps, where "unnecessary" means that the proof of security doesn't require them. Never mind that HMQV as published in Crypto 2005 was insecure, because of the omitted step. Never mind that its "rigorous mathematical" proof of security was fallacious.

Why do prominent researchers react so angrily to criticism? Why do they expect everyone to think that they are perfect and never make mistakes? Is it because of their personalities? Do they behave this way in the non-crypto world with their families and friends? My guess is they don't. They probably have pleasant, normal personalities in the outside world, and the reason for their behavior in the crypto world is that our disciplinary culture tolerates and even encourages bad behavior.

5 Harmful Effects

Have Menezes and I suffered reprisals for our "Another Look" series of papers? For example, have Bellare's colleagues who "reacted violently to every paper in the series" sometimes blocked (or attempted to block) publication of our work? Of course. But that does us no harm really, because we can easily find ways around it — and in any case we're established old guys with secure jobs in university math departments. So there's not much they can do except wallow in impotent rage.

The harmful effects of the aggressive behavior and angry reaction to criticism are felt most of all in the younger generation of recent PhDs who are starting out and have no job security. They are pressured to conform, are socialized into a sycophantic attitude toward the old guys, and are less likely to challenge

reigning paradigms and go in radically new directions. The message to young people is a new KISS principle: Kiss up to the establishment, flatter your elders, do what they say, and *never, never* criticize them. This is not the way that science progresses.

There's another harmful effect of our disciplinary culture that concerns me: it discourages most women. In almost all cultures of the world, women from a young age are socialized into thinking that aggressive competitiveness and excessive boasting are improper behavior for women. Even when they see men behaving that way, they grow up with the understanding that such male behavior is wrong for them. Plenty of men also find a hyper-competitive, egotistical disciplinary culture to be unpleasant. But on average women are even more likely to find it disagreeable.

In the U.S., this is reflected in the statistics about female participation in computer science (from which we inherited our disciplinary culture) versus mathematics (which has a less competitive disciplinary culture). In the 1970s and 1980s, when the young field of computer science had a very different disciplinary culture from what it has now, there was a higher percentage of women studying at an advanced level in computer science than in mathematics. However, at present roughly 30% of math PhDs go to women, whereas women get only about 20% of computer science PhDs. Although no one intended to discriminate against women, our disciplinary culture in effect does precisely that.

6 Conclusion

In our time — especially since January 2017 — irrational and vindictive behavior, unrestrained boastfulness, and rejection of well-established norms of scientific inquiry are being more and more associated with American national character. When certain prominent U.S.-based cryptographers react angrily to technical criticisms of their work, retaliate against their critics, and continue to hype their work without mentioning the flaws or weaknesses that have been discovered, they are conforming to this unfortunate stereotype of Americans.

It is time for our community to return to the scholarly values that were articulated in the ancient world, for example, by the great leader of Islam of the 7th century, Ali Ibn Abi Talib, who said

> The most harmful disaster for the intellect is arrogance.

And also:

> When proven wrong, the wise man will correct himself and the ignorant will keep arguing.

We need to make a paradigm shift in our disciplinary culture before we can claim that our field deserves to be called a "science." We should agree to use words like "scientist" and "scholar" only for those who

- present their results modestly and honestly, highlighting the limitations and never overstating their accomplishments; and

• respond to criticism by thanking the critics and withdrawing any claims that are shown to be fallacious or questionable.

We should use words like "marketer" and "hypester" for those who
• make exaggerated or misleading claims in their abstract or introduction;
• engage in aggressive self-promotion; or
• respond to critics with anger and retaliation, rather than carefully addressing the technical issues that the critics have raised.

References

1. L. Adleman, J. DeMarrais and M. Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields, *Algorithmic Number Theory: First International Symposium*, LCNS 877, Springer-Verlag, 1994, pp. 28-40.
2. M. Bellare, New proofs for NMAC and HMAC: Security without collision-resistance, *Advances in Cryptology – Crypto 2006*, LNCS 4117, Springer-Verlag, 2006, pp. 602-619.
3. M. Bellare, email to N. Koblitz, 24 February 2012.
4. S. Blake-Wilson and A. Menezes, Unknown key-share attacks on the station-to-station (STS) protocol, *Public Key Cryptography – PKC 1999*, LNCS 1560, Springer-Verlag, 1999, pp. 156-170.
5. S. Chatterjee, N. Koblitz, A. Menezes, and P. Sarkar, Another look at tightness. II, this volume.
6. 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*, 1984, pp. 441-448.
7. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman and Hall/CRC, 2007.
8. N. Koblitz, The uneasy relationship between mathematics and cryptography, *Notices of the Amer. Math. Soc.*, **54** (2007), pp. 972-979.
9. N. Koblitz and A. Menezes, Another look at HMAC, *J. Mathematical Cryptology*, **7** (2013), pp. 225-251.
10. N. Koblitz and A. Menezes, Another look at security definitions, *Advances in Mathematics of Communications*, **7** (2013), pp. 1-38.
11. N. Koblitz and A. Menezes, Another look at security theorems for 1-key nested MACs, *Open Problems in Mathematics and Computational Science*, 2014, pp. 69-89.
12. H. Krawczyk, HMQV: A high-performance secure Diffie-Hellman protocol, *Advances in Cryptology – CRYPTO 2005*, LNCS 3621, Springer-Verlag, 2005, pp. 546-566.
13. A. Menezes, Another look at HMQV, *J. Mathematical Cryptology*, **1** (2007), pp. 47-64.
14. A. Menezes, T. Okamoto and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transactions on Information Theory*, **39** (1993), pp. 1639-1646.
15. S. Micali and L. Reyzin, Physically observable cryptography, *First Theory of Cryptography Conference – TCC 2004*, LNCS 2951, Springer-Verlag, 2004, pp. 278-296.

16. G. M. Zaverucha, Hybrid encryption in the multi-user setting, available at http://eprint.iacr.org/2012/159.pdf.