16-bit AES.

17 slides for a 3-minute rump session talk.

2 to 4 kilograms of top quality amphetamines.

2-sentence Eurocrypt reviews.

4mm reasonable margins.

A 25-year old policy on sexual harassment.

A Facebook friend request from a cryptographer I actually despise.

A career-limiting card game.

A dancing cryptographer.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

A genuine attempt to configure IPsec.

A hand wavy argument.

A long-term nonce.

A non-fabricated use of pairings.

A painfully slow Tor masturbation session.

A popup Skype notification from “lovemachine69” during my keynote talk.

A proof that appears in the “full version”.

A shepherd that won’t budge.

A tight security reduction to the problem of fending off a sexually voracious goat.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

A violent and bloody PhD defence.

Aaron Aaronson’s insistence on alphabetical author ordering.

Academic integrity.

Accidentally sexting my co-supervisor.

Actually being “sorry for the late reply”.

Actually efficient indistinguishability obfuscation.

Adleman-Rivest-Shamir encryption (the ARSE algorithm).

An IACR board meeting.

An SSL vulnerability with a silly name.

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

An “anonymous” reviewer insisting I cite 6 papers by the same author.

An inappropriate workplace romance.

An insecure VPN straight to the Kremlin.

An overfull hbox.

An overlooked patent.

Arriving 13 minutes late to a 15 minute talk and having the gall to ask a question.

Asking for 2 room keys during check-in, knowing full well I’m not getting laid.

Bart Preneel’s private key.

Beefing up my Proposition to a Theorem because I’m that awesome.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Being forced to attend social events because I’m the visitor’s official host.

Being the only smartly dressed person in the room.

Best rejected paper award.

Bragging about getting held up at Border Control for saying I’m a cryptographer.

Brexit.

Checking my Google Scholar profile daily.

Chocolate-covered shrimp.

Citing personal communication.

Conferences with 5 submissions at 11:59pm.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Crippling student debt.

Crypto wars.

Deadline day flatulence.

Deliberately hiding inefficiencies inside the big O.

Deliberately not referencing a superior paper.

Diffie but definitely not Hellman.

Doing Facebook maths puzzles to show I am better than those idiot 97%.

Double ROT-13.

Drinking alone.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Dropping the word Blockchain into my research proposal as many times as possible.

Dual_EC_DRBG.

Encrypted database security definitions.

Explaining what my job is at a family reunion.

Falling asleep in a 5-person meeting.

Feeling flattered because a conference spam email addressed me as Professor.

Fighting over LaTeX syntax.

Filing a patent application for modular multiplication... in 2017.

Flirting with people at the conference registration desk.

Cards Against Cryptography

Cards Against Cryptography

Cards Against Cryptography

Cards Against Cryptography

Cards Against Cryptography

Cards Against Cryptography

Cards Against Cryptography

Cards Against Cryptography

Cards Against Cryptography

Forgetting my VGA adapter.

Frantically taking notes during every talk.

GDPR requirements.

Getting a fourth cookie during a coffee break because I have no one to talk to.

Getting rejected, but then taking immediate solace in the fact that the selection of papers was a difficult and challenging task.

Getting stuck at the French-speaking banquet table.

Getting tenure, then chilling the f— right out!

Getting turned on by a proof.

Going straight to journal.

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

Government-mandated backdoors.

HTTPS everywhere!

Hands-on supervision.

Having to write a polite rebuttal to the reviewer who clearly didn't read past page 2.

Hiding my conflict of interest.

Hillary Clinton's BlackBerry.

Home-baked, snake oil crypto.

Ignoring reviewer comments and resubmitting immediately.

Ignoring the session chair flashing 5 minutes left because I've got 23 slides to go.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Including an XKCD comic in my slides because I’m so original.

Knapsack cryptosystems, revisited.

LNCS’ 25-foot margins.

Making claims in the submission that you hope you can achieve before the rebuttal.

Maths-terbation.

My Silk Road purchase history.

My *h*-index.

My automated reply saying “email responses will be delayed”, when I know damn well I’ll be online with high-speed internet access 24/7.

My butt.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

My crypto blog views getting into the double digits.

My dear friend the Program Chair overruling 3 borderline rejects on my paper.

My genitals.

My inappropriate supervisor.

My inflated sense of self-importance that warrants my PGP key.

My much more successful career as a singer after rocking the Crypto rump session.

My relationship status.

My second divorce.

My sex life.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

My side job as an incompetent security consultant.

My successful career at a patent troll company.

My supervisor’s morning breath.

Nigel Smart’s new Hawaiian shirt.

Overselling it hard in the introduction.

Password1.

Picturing the FSE audience naked.

Politely starting an answer with “That’s a good question...”, when the question is actually idiotic.

Post-quantum RSA.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Preparing for two weeks to give a 15-minute presentation to a room of 7 people all on their laptops.

Pretending to care when my vegetarian coauthor complains about the lack of banquet options.

Pretending to understand.

Pubic key cryptography.

Publishing anyway.

Purchasing the Springer hardcopies I publish in because my mom is collecting them.

Putting an outdoors-y photo on my academic webpage to look well-rounded.

Quadruple XOR.

Quantum key distribution.

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

Quickly trying to peek at someone’s badge as I shake their hand, but it’s flipped backwards.

Reading the person in front’s emails.

Relatives who ask me to help them install their printer on Windows.

Rogaway’s loose morals.

Satoshi Nakamoto.

Security through obscurity.

Sending an email at 11pm so people think I work hard.

Serious rump session speakers.

Sexual tension.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Skype dropping out every 10 to 15 seconds.

Social sciences.

Someone less senior than me signing off with “Thanks in advance”.

Spending 3 Bitcoin on pizza in 2012.

Spending all of my Levchin prize money on cocaine.

Springer’s editorial team.

Starting a conversation with “When did you fly in?”, because I have nothing interesting to say.

Taking a group shower with my recent co-authors.

Telling anyone who’ll listen quite how busy I am.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Thanking the anonymous reviewers for their “useful” comments.

That feeling when my article is sitting pretty at the top of the ePrint archive.

That one asshole who’s always sleeping during my Eurocrypt talks.

The MIT Mafia.

The NSA’s massive stack of amateur porn.

The North Korean Cryptographic Standard.

The awkward question the chair asks when nobody understood the talk.

The awkward silence of 8 people standing in a circle during the afternoon coffee break.

The great firewall of China.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

The great paywall of IEEE.

The intoxicating aroma of 12 PhD students in one office.

The latest dance mix album by DJ Bernstein.

The one person I don’t want to get stuck next to on the conference excursion bus.

The one really hot person at CHES registration drinks.

The one suit I own for meetings with industry.

The person in the front row taking photos of every slide.

The secret flash drive hidden in my underwear.

The student body.

Cards Against Cryptography	**Cards Against Cryptography**	**Cards Against Cryptography**
Cards Against Cryptography	**Cards Against Cryptography**	**Cards Against Cryptography**
Cards Against Cryptography	**Cards Against Cryptography**	**Cards Against Cryptography**

The walking zombie corpse of Claude Shannon.

Thinking I’m so clever for using pictures of Alice (Cooper) and Bob (Marley).

Throwing a party for my next citation milestone.

Trying to make TCC friends at the bar in order to get the IACR 7-conference grand slam.

Turbulent bowel movements in the middle of my Asiacrypt presentation.

Turning up to one meeting and claiming co-authorship.

Tweeting about my paper acceptance.

Unbreakable military-grade encryption.

Undergrads.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Using Beamer because it’s social suicide to use PowerPoint.

Using “it clearly follows” when the implied following is anything but clear.

Using “we should talk about this offline” because the question exposes holes in my paper.

Using indecipherable, non-standard notation to hide a dodgy proof.

Vital sugar beet auctions.

WalnutDSA.

Wearing a T-shirt with a Linux joke.

Wearing a conference t-shirt... in public.

When you realize that quantum computers have been 10 years away for 3 decades.

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Cards
Against
Cryptography

Wistfully looking out of the window of my overly-cramped PhD office.

Writing a reference for someone I can't remember meeting.

Yet another cryptographer falling into the blockchain startup abyss.

`Ctrl+F`**'ing to see how many times I'm cited and finding "0 results".**

"Working" remotely.

A slide deck entirely in Comic Sans.

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**