| | | |
|---|---|---|
| **A slide deck entirely in Comic Sans.**  | **`Ctrl+F`'ing to see how many times I'm cited and finding "0 results".**  | **"Working" remotely.**  |
| **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.**  |

| | | |
|---|---|---|
| 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 career-limiting card game.**  | **A dancing cryptographer.**  | **A genuine attempt to configure IPsec.**  |
| **A hand wavy argument.**  | **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.**  |

| | | |
|---|---|---|
| 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 |

| | | |
|---|---|---|
| **Aaron Aaronson's insistence on alphabetical author ordering.**  | **Accidentally sexting my co-supervisor.**  | **Actually being "sorry for the late reply".**  |
| **Actually efficient indistinguishability obfuscation.**  | **Adleman-Rivest-Shamir encryption (the ARSE algorithm).**  | **An "anonymous" reviewer insisting I cite 6 papers by the same author.**  |
| **An IACR board meeting.**  | **An insecure VPN straight to the Kremlin.**  | **An overfull hbox.**  |

| | | |
|---|---|---|
| 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 SSL vulnerability with a silly name.**  | **Arriving 13 minutes late to a 15 minute talk and having the gall to ask a question.**  | **Beefing up my Proposition to a Theorem because I'm that awesome.**  |
| **Best rejected paper award.**  | **Brexit.**  | **Checking my Google Scholar profile daily.**  |
| **Chocolate-covered shrimp.**  | **Citing personal communication.**  | **Crippling student debt.**  |

| | | |
|---|---|---|
| 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 |

| | | |
|---|---|---|
| **Crypto wars.**  | **Deliberately hiding inefficiencies inside the big O.**  | **Deliberately not referencing a superior paper.**  |
| **Diffie but definitely not Hellman.**  | **Double ROT-13.**  | **Drinking alone.**  |
| **Dropping the word Blockchain into my research proposal as many times as possible.**  | **Encrypted database security definitions.**  | **Explaining what my job is at a family reunion.**  |

| | | |
|---|---|---|
| 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 |

| | | |
|---|---|---|
| **Fighting over LaTeX syntax.**  | **Filing a patent application for modular multiplication... in 2017.**  | **Forgetting my VGA adapter.**  |
| **Frantically taking notes during every talk.**  | **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.**  |

| | | |
|---|---|---|
| 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 |

| | | |
|---|---|---|
| **Going straight to journal.**  | **Having to write a polite rebuttal to the reviewer who clearly didn't read past page 2.**  | **Hillary Clinton's BlackBerry.**  |
| **Home-baked, snake oil crypto.**  | **HTTPS everywhere!**  | **Ignoring reviewer comments and resubmitting immediately.**  |
| **Ignoring the session chair flashing 5 minutes left because I've got 23 slides to go.**  | **Including an XKCD comic in my slides because I'm so original.**  | **Knapsack cryptosystems, revisited.**  |

| | | |
|---|---|---|
| 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 |

| | | |
|---|---|---|
| **LNCS' 25-foot margins.**  | **Making claims in the submission that you hope you can achieve before the rebuttal.**  | **Maths-terbation.**  |
| **My *h*-index.**  | **My butt.**  | **My genitals.**  |
| **My inappropriate supervisor.**  | **My relationship status.**  | **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 Silk Road purchase history.**  | **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 understand.**  | **Publishing anyway.**  |
| **Putting an outdoors-y photo on my academic webpage to look well-rounded.**  | **Quadruple XOR.**  | **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.**  |

| | | |
|---|---|---|
| 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 |

| | | |
|---|---|---|
| **Satoshi Nakamoto.**  | **Sending an email at 11pm so people think I work hard.**  | **Sexual tension.**  |
| **Skype dropping out every 10 to 15 seconds.**  | **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.**  |

| | | |
|---|---|---|
| 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 |

| | | |
|---|---|---|
| **Telling anyone who'll listen quite how busy I am.**  | **Thanking the anonymous reviewers for their "useful" comments.**  | **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.**  | **The great paywall of IEEE.**  |
| **The intoxicating aroma of 12 PhD students in one office.**  | **The North Korean Cryptographic Standard.**  | **The NSA's massive stack of amateur porn.**  |

| | | |
|---|---|---|
| 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 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 walking zombie corpse of Claude Shannon.**  | **Thinking I'm so clever for using pictures of Alice (Cooper) and Bob (Marley).**  |
| **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.**  |

| | | |
|---|---|---|
| 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 |

| | | |
|---|---|---|
| **Unbreakable military-grade encryption.**  | **Undergrads.**  | **Using "it clearly follows" when the implied following is anything but clear.**  |
| **Using Beamer because it's social suicide to use PowerPoint.**  | **Using indecipherable, non-standard notation to hide a dodgy proof.**  | **Vital sugar beet auctions.**  |
| **Wearing a conference t-shirt... in public.**  | **Wistfully looking out of the window of my overly-cramped PhD office.**  | **Writing a reference for someone I can't remember meeting.**  |

| | | |
|---|---|---|
| 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 |