Titles count ...so... count Titles!

CHES 2015 Rump Session

Alberto Battistello and Christophe Giraud(y)

September 14, 2015
"The title should be as informative as possible and yet not too cumbersome or too long."
5 Pretty Good Examples

- "Slide Attacks"
- "Certifying RSA"
- "Identity Escrow"
- "Group Signatures"
- "Crypto-integrity"
However, “not too long” is prone to interpretations...
"Improving Non-Profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-Channel High-Resolution EM Measurements" - 16w

"Finding Small Solutions of a Class of Simultaneous Modular Equations and Applications to Modular Inversion Hidden Number Problem and Inversive Congruential Generator" - 22w

"Achieving a log(n) Speed Up for Boolean Matrix Operations and Calculating the Complexity of the Dense Linear Algebra step of Algebraic Stream Cipher Attacks and of Integer Factorization Methods" - 29w

"David & Goliath Oblivious Affine Function Evaluation - Asymptotically Optimal Building Blocks for Universally Composable Two-Party Computation from a Single Untrusted Stateful Tamper-Proof Hardware Token" - 24w
"Improving Non-Profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-Channel High-Resolution EM Measurements" - 16w
- "Improving Non-Profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-Channel High-Resolution EM Measurements" - 16w
- "Finding Small Solutions of a Class of Simultaneous Modular Equations and Applications to Modular Inversion Hidden Number Problem and Inversive Congruential Generator" - 22w
▶ "Improving Non-Profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-Channel High-Resolution EM Measurements" - 16w

▶ "Finding Small Solutions of a Class of Simultaneous Modular Equations and Applications to Modular Inversion Hidden Number Problem and Inversive Congruential Generator" - 22w

▶ "Achieving a log(n) Speed Up for Boolean Matrix Operations and Calculating the Complexity of the Dense Linear Algebra step of Algebraic Stream Cipher Attacks and of Integer Factorization Methods" - 29w
"Improving Non-Profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-Channel High-Resolution EM Measurements" - 16w

"Finding Small Solutions of a Class of Simultaneous Modular Equations and Applications to Modular Inversion Hidden Number Problem and Inversive Congruential Generator" - 22w

"Achieving a log(n) Speed Up for Boolean Matrix Operations and Calculating the Complexity of the Dense Linear Algebra step of Algebraic Stream Cipher Attacks and of Integer Factorization Methods" - 29w

"David & Goliath Oblivious Affine Function Evaluation - Asymptotically Optimal Building Blocks for Universally Composable Two-Party Computation from a Single Untrusted Stateful Tamper-Proof Hardware Token" - 24w
Conclusion

Longer words makes titles asymptotically longer!
Conclusion

Longer words makes titles asymptotically longer!

While long titles may be appealing, we suggest that they should keep in a single big breath.